COMPUTER SEIZURE AS TECHNIQUE IN FORENSIC INVESTIGATION

By

VUYANI NDARA

Submitted in partial fulfillment of the requirements for the degree of

MAGISTER TECHNOLOGIAE

In the subject

FORENSIC INVESTIGATION

At the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: Ms JS HORNE

C0-SUPERVISOR: Ms M VAN ZYL

FEBRUARY 2013

ABSTRACT

The problem encountered by the researcher was that the South African Police Service Cyber-Crimes Unit is experiencing problems in seizing computer evidence. The following problems were identified by the researcher in practice: evidence is destroyed or lost because of mishandling by investigators; computer evidence is often not obtained or recognised, due to a lack of knowledge and skills on the part of investigators to properly seize computer evidence; difficulties to establish authenticity and initiate a chain of custody for the seized evidence; current training that is offered is unable to cover critical steps in the performance of seizing computer evidence; computer seizure as a technique requires specialised knowledge and continuous training, because the information technology industry is an ever-changing area.

An empirical research design, followed by a qualitative research approach, allowed the researcher to also obtain information from practice. A thorough literature study, complemented by interviews, was done to collect the required data for the research. Members of the South African Police Cyber-crime Unit and prosecutors dealing with cyber-crime cases were interviewed to obtain their input into, and experiences on, the topic.

The aim of the study was to explore the role of computers in the forensic investigation process, and to determine how computers can be seized without compromising evidence. The study therefore also aimed at creating an understanding and awareness about the slippery nature of computer evidence, and how it can find its way to the court of law without being compromised. The research has revealed that computer crime is different from common law or traditional crimes. It is complicated, and therefore only skilled and qualified forensic experts should be used to seize computer evidence, to ensure that the evidence is not compromised. Training of cyber-crime technicians has to be priority, in order to be successful in seizing computers.

Key Terms:

Forensic; Digital forensic; Computer; Digital evidence; Investigators; Technicians; Chain of custody; Seizure; Cyber-crime; Cyber-crime technicians

ACKNOWLEDGEMENTS

God is love – how wonderful are the things He does.

To my supervisor, Mrs Juanida Horne, thank you for your encouragement and guidance. My co-supervisor, Mrs Marielize van Zyl, your fine and excellent approach has been a beacon of hope to me. Your worthwhile contribution in developing this country academically is the value attached to you by our mighty God.

To my colleague, Warrant Officer Dalene Webb, I am really grateful for your assistance in compiling this research study, God bless those hands.

To all the participants who willingly supported me with the interviews, God is love.

To my lovely wife Ncedisa, and kids Siphe, Ubom and Ngokwedingalakho, thank you for the time you have given me to further my studies.

DECLARATION

I declare that this research dissertation, submitted in partial fulfillment of the requirements for the degree MTech: Forensic Investigation, at the University of South Africa, Student number 34722491, represents my own work, and every source used or quoted has been reflected and acknowledged by means of complete references.

……

VUYANI NDARA

2013-02-20

TABLE OF CONTENTS

CHAPTER 1
GENERAL ORIENTATION

1.1 INTRODUCTION

According to Welman, Kruger and Mitchell (2005:13), a problem statement is the result of focusing specifically on a particular problem which is interesting and necessary to be investigated or researched. Before the problem with regard to computer seizure is addressed, it is important to understand what a computer is. O'Brien and Marakas (2009:625) define a computer as "a device that has the ability to accept data; internally store and execute a program of instructions; perform mathematical, logic, and manipulative operations on data; and report the results". This view is supported by *Computer Dictionary*, (2010), the program defines a computer as a general purpose device that can be programmed to carry out a finite set of arithmetic or logic operations. A "computer" is an electronic device which is capable of storing and processing information in accordance with a set of instructions, as explained by the (*South African Pocket Oxford Dictionary*, 2002:177). From this explanation it is clear that information forms an important aspect of computers.

Bologna (1989:1) points out that in computer crimes such as fraud, larceny, embezzlement, sabotage of equipment or information theft, it is usually a matter which is left to forensic experts to investigate. The author further argues that investigators of computer crimes must therefore have at least a general knowledge of accounting, and also auditing principles and techniques, including some understanding of how computers operate with respect to the recording of financial transactions and financial information.

According to Casey and Ferraro (2005:195), computer or cyber forensics involves the identification, extraction, documentation, interpretation and preservation of electronic data, whose eventual disposition may be used as evidentiary material in a court of law. Davis, Philipp and Cowen (2005:58) further believe that seizure of computer evidence is the most important part of the investigation. It does not matter how good the analysis and procedures are. If the

evidence seized is not collected in a forensically sound matter, all the hard work will not hold up and will be wasted. Casey (2002:367) supports the view that investigators should ensure that they follow an acceptable procedure for properly seizing and storing electronic evidence. Anson and Bunting (2007:15) add how critical and how difficult seizing computers can be, and also getting all the evidence that can be physically hidden somewhere, only to lose it due to its fragile nature. Cross (2008:2) believes that although the cyber-crime phenomenon has grown in recent years, many information technology (IT) and law enforcement professionals lack the necessary tools and expertise to address the problem of cyber-crime investigations.

Burrows (2009) explain that the South African Police Service (SAPS) Cyber-crime Unit resorts under crime intelligence divisions which are situated all over the country. It has nine offices in eight provinces, supporting functional policemen with cyber-crime related matters. North West is the only province without an office. There are currently 43 cyber-crime technicians dealing with cyber-crimes in the country.

Afrika, (2009) gives a brief but sharp analysis of crime statistics released by South African Business Against Crime in July 2008. Incidences of commercial crimes, under which cyber-crimes fall, had risen by 13% to 61690 per 100 000 people between 2007 and 2008. In the same article, the banks are quoted as saying that they have had only a few successes, working with the South African Police Service (SAPS), in solving cyber-crimes. In the same article, the two banks were quoted as follows:

- Forrester (in Africa, 2009) who is the security analyst of Standard Bank has been quoted saying that the bank has run to “some dead ends” with the police in phishing scam investigations.
- First National Bank (FNB) spokesman, Higgins (in Africa, 2009) said that the bank uses its own forensic team to investigate cyber-crimes, and hands the evidence over to the police.

Afrika, (2009) further points out that Weertman (in Africa, 2009) who attended a meeting in Johannesburg during April 2009, believed that the police do not have the necessary capacity to

investigate cyber-crime. In this same article it was argued that training in cyber-crime is costly, and heavy reliance has to be placed on assistance from the private sector and international donors.

From the abovementioned statements, it is quite evident that the SAPS is experiencing problems in dealing with computer evidence. For argument's sake, why would FNB use its own forensic team and hand over the evidence to the police, after the criticism that the police do not have the capacity to investigate cyber-crimes? It is also confirmed by many authors that seizing computers is the most difficult stage of the investigation process. Fisher (2004:193) explains that some of the ways computer evidence is destroyed is from mishandling seized equipment. The fragile nature and volatility of computer evidence requires specialised knowledge. If this type of evidence cannot be seized properly, there will be no cases to be dealt with.

Based on his practical work experience, the researcher understands that there are problems with regard to the seizure of computer evidence. The following problems were identified by the researcher, in practice:

- Computer evidence is destroyed or lost because of mishandling by investigators.
- Computer evidence that is not obtained or recognised, due to a lack of knowledge and skills of investigators to properly seize computer evidence.
- Difficulties in establishing authenticity, and initiating a chain of custody of the seized computer evidence.
- Current training being offered does not cover critical steps in the process of seizing computer evidence.

Computer seizure as a technique requires specialised knowledge and continual training, because the IT industry is an ever-changing environment. These problems can have a very negative effect on the outcome of an investigation where computer evidence is needed to prove a case. In order to address the problems regarding the seizure of computer evidence, the researcher has identified an urgent need for research on proper procedures to follow.

1.2 RESEARCH AIMS

The researcher's aim is to determine procedures for the seizure of computers in a forensic investigation, without compromising evidential value.

The main aim is to develop proper procedures that can be followed when computers are seized during a forensic investigation. The researcher's recommendations are aimed at improving the seizure of computers as a technique in investigation.

1.3 PURPOSE OF THE RESEARCH

Denscombe (2002:24) states that the purpose of the research provides researchers with answers to what they want to achieve. Maxfield and Babbie (1995:70) further explain that research can have more than one purpose – such as exploration, explanation, description, application, prediction and empowerment. The researcher studied all these purposes, and determined that the purpose of this research is application to improve procedures with regard to seizure of computer evidence. According to Denscombe (2002:27), application focuses on developing good practice – in other words, how a procedure can be improved (in this case, the seizure of computers).

Another research purpose is to imbue those who are being researched, with the knowledge and skills to effectively seize computers during the investigation of cyber-crimes. In this regard, it is all role-players involved in the investigation of computer crime, but, more specifically, cyber-crime technicians, who will benefit from a well-researched procedure that can be followed during computer investigations.

1.4 RESEARCH QUESTIONS

The purpose of research questions is to explain clearly what the researcher has identified, the reason for the research, and what will be investigated by the research (Denscombe, 2002:31). The following research questions will guide the researcher in solving the complexity of computer seizure:

- What is the role of a computer in facilitating the commissioning of an offence, in forensic investigation? How can computers be seized without compromising evidence?

1.5 DEMARCATION

The researcher would like to inform readers that information in the research study overlaps or continues from one chapter to the next. The reason for this is to have collaboration, and be cogent of the text. Another important aspect is the use of the word 'role' in the title of Chapter 2 – it means the role of a computer in forensic investigation. The reason for this is to introduce the readers to another perspective on the use of a computer. In a general sense, a computer replaces pen and paper, and is also used for storing information. On the other hand, this valuable device is used in the commissioning of crime. This is the unknown part, to many members of society. The word 'role' is used to indicate the part it plays in the act of crime, due to its existence.

1.6 KEY THEORETICAL CONCEPTS

According to Leedy and Ormrod (2001:119), key theoretical concepts prevent misunderstanding or confusion on the part of other researchers or readers that may arise in future. For the purpose of this study, the researcher adopted the following definitions:

1.6.1 Forensic

Axelrod and Antinozzi (2003:170) define 'forensic' as "the use of scientific methods, procedures and equipment to investigate crimes to prove in a court of law the guilt of the accused person(s)".

1.6.2 Digital forensics

Casey and Ferraro (2005:73) explain that the term 'digital forensics' refers to the "study of technology, the way criminals use it, and the way to extract and examine digital evidence".

1.6.3 Computer

According to the (*South African Pocket Oxford Dictionary*, 2002:177), "a computer is an electronics device capable of storing and processing information in accordance with a set of instructions".

1.6.4 Digital evidence

Casey and Ferraro (2005:12) define ‘digital evidence as any data stored or transmitted using a computer that supports or refutes a theory of how an offence occurred or that addresses a critical element of the offence such as intent or alibi”.

1.6.5 Investigators

Kipper (2007:55) describes investigators in computer crime as "people who handle nuts and bolts of the digital evidence by managing the preservation, acquisition, examination, analysis and reporting”.

1.6.6 Technicians

“Technicians are trained to seize electronic equipment and digital images properly” (Kipper, 2007:55).

1.6.7 Chain of custody

According to Fisher (2004:11), a “chain of custody shows who had contact with the evidence, at what time, under what circumstances, and what changes, if any, were made to the evidence”.

1.6.8 Seizure

“Seizure is an action of seizing, which refers mainly to officially taking possession of something” (*South African Pocket Oxford Dictionary*, 2002:814).

1.6.9 Cyber-crime

Casey and Ferraro (2004:667) define cyber-crime “as any offense where the modus operandi or signature involves the use of a computer network in any way”.

1.6.10 Cyber-crime technicians

In the view of the researcher, cyber-crime technicians are both technicians and investigators, because they manage the preservation, acquisition, examination, analysis and reporting, and seize electronic equipment.

1.7 RESEARCH DESIGN

According to Mouton (1996:175), a research design is that detailed plan by the researcher to carry out an investigation into the research problem. Singleton and Straits (1999:91) argue that a research design is composed of an unambiguous statement of the research problem, as well as the means of collecting, actions towards achieving the result, and interpreting what has been observed, with the aim of providing solutions to the problem. In addition to this, De Vos (2002:120) describes a research design as a "blue print or detailed plan the researcher has to follow in conducting and operationalising variables so that it could be measured, selected samples to the study, collecting data and analyzing the results".

The researcher decided to make use of an empirical research design for this study, because it is the kind of research that allows the researcher to go out of the office and gather information directly from people as Denscombe (1998:6) explains: obtaining information "straight from the horse's mouth". The researcher therefore produced data based on real-world scenarios and the practical field experience of the SAPS cyber-crime members, in order to answer the research questions.

1.8 RESEARCH APPROACH

According to Mouton (1996:169), a qualitative research approach is explorative, descriptive and contextual in nature; it therefore allows a researcher to interview participants with the view to obtaining information from their personal experience. There was a need to go out and seek information in the field, because there is not much written on it. The researcher decided to go out and seek information from the SAPS cyber-crime technicians, about the complex problem of seizing computer evidence. The qualitative research approach was used to conduct interviews with members of the SAPS Cyber-crime unit to obtain first-hand information on the topic. State prosecutors were interviewed to obtain their views on the topic. De Vos (2002:79) also agrees that the qualitative approach is most suitable to obtain first-hand information from participants on the research problem.

1.9 TARGET POPULATION

Maxfield and Babbie (1995:185) define 'population' as a "theoretically specified aggregation of study elements". Hoyle, Harris and Judd (2002:8) support the view that a population is the aggregate of all the specified elements to be studied. According to Welman and Kruger (2001:119), a target population is most suitable for the researcher to make a broad statement about the results of the research study. The population for the purpose of the study consists of the 43 SAPS cyber-crime technicians presently in eight of the provinces of South Africa. There are 14 members in Gauteng, 14 in the Western Cape, three in the Eastern Cape, two in the Free State, three in Mpumalanga, three in KwaZulu-Natal, two in the Northern Cape, and two members in Limpopo. This is a small population, so the researcher chose to make use of the whole population. Limitations with regard to the interviews with the police cyber-crime technicians are thoroughly discussed in section 1.11.2, on interviews. For this reason, the findings of this research cannot be generalised and are only applicable to the participants who were interviewed in this research.

However, all SAPS Cyber-crime technicians were requested to participate in the research study from all the provinces as indicated above.

1.10 SAMPLING

Blaikie (2003:161) defines a sample as "a selection of elements (members or units) from a population and is used to make statements about the whole population". Leedy and Ormrod (2001:211) explain that sampling refers to that carefully chosen portion that, in the eyes of a researcher, will present the characteristics of the whole population.

The population of SAPS cyber-crime technicians is so small, that the researcher decided not to draw a sample but to use the whole population for the purpose of this study. A purposive or judgmental sampling method was used, as explained by Welman and Kruger (2001:63), to sample the five senior state prosecutors. The reason for using this sampling method was that it enabled the researcher to hand-pick the participants on the basis of their specific knowledge of, and experience in, the topic.

The three state prosecutors interviewed were from Port Elizabeth. Silvermand (2000:104) points out that "purposive sampling allows researchers to choose a case because it illustrates some features or process in which researchers are interested". Prosecutors have particular knowledge of the investigation and prosecution process; therefore, they could cover every technical point that might arise with regard to the legal framework of seizing computers. Leedy and Ormrod (2005:206) also believe that "in purposive sampling, people or other units are chosen, as the name implies, for a particular purpose." In this case, the purpose was to obtain the experience of the state prosecutors in dealing with computer evidence. Limitations with regard to interviewing the SAPS cyber-crime technicians and prosecutors are discussed in the section on interviews – section 1.11.2.

1.11 DATA COLLECTION

Bauer and Gaskell (2000:355) define data "as facts or evidence that are at the disposal of the proponent of an argument". Bouma and Atkinson (1995:22) are also of the view that data can also be regarded as facts. They comment that data "are records of the actual state of some aspect of the universe at a particular point of time".

Data collection is the stage where researchers consider a method which is most appropriate in the light of their research problem and the population in question (Welman & Kruger, 2001:127). The most common data collection methods are the following: observation, interviewing, physical sources and archival and or documentary sources. The researcher made use of a literature study and interviews, to obtain information on the research problem. A docket analysis was not considered, because it would have been too difficult to identify relevant case dockets.

1.11.1 Literature

Denscombe (2002:51) argues that literature is very important in data collection, to give the researcher the context of the published knowledge about a research topic. In addition to this, the literature review will show if the current research has something to offer. Different views of authors were discussed, integrated and critically analysed to place the current research within a conceptual and theoretical context.

National and international information sources that were used were as follows: academic books, academic journal articles, newspaper articles, national instructions, SAPS manuals, SAPS publications, SAPS circulars, laws/acts and statutes, theses and dissertations, conference proceedings, policy documents, and information available on the Internet. The aims and research questions served as a guide to trace relevant literature on the topic.

1.11.2 Interviews

Leedy and Ormrod (2005:185) believe that personal interviews, whether they are face-to-face or over the telephone, give an opportunity to gain a good understanding of the situation. De Vos (2002:289) emphasizes that interviews are used to determine the perceptions, opinions, facts, and interviewee reactions. Robson (2000:88) states that there are three broad styles of conducting interviews, namely: informal interviews, semi-structured interviews, and structured interviews. Babbie and Mouton (2002:289) explain that interviewing is a method used to collect data in a qualitative research approach. The researcher made use of structured interviews. According to Robson (2000:90), a structured interview is a fixed sequence of predetermined questions which are easily compared, with less risk of being biased, on the part of the researcher. In addition to this, Leedy and Ormrod (2005:184) believe that in structured interviews the researcher asks a standard set of questions. A compiled questionnaire, known as an interview schedule, was used to interview the participants. The interview schedule conducted with the cyber-crime technicians is attached as Annexure A and the interview schedule conducted with the prosecutors is attached as Annexure B. According to Welman and Kruger (2001:160), it is vital that the interviewer be restricted to the questions, their wording, and their order as they appear on the schedule, with relatively little freedom to deviate from it.

The researcher used both face-to-face and telephone interviewing methods to conduct the interviews. According to Leedy and Ormrod (2005:184), face-to-face interviews produce the highest response, and also having the advantage of helping the researcher to obtain the full cooperation of the potential participant in establishing a rapport. However, telephonic interviews

were conducted to cover the vast geographic area involved, to avoid travelling costs and to speed up the process. For telephonic interviews, an e-mail with the interview schedule attached was forwarded to the participants before the interviews were conducted. This ensured that the questions were clear and in front of them when the researcher interviewed them over the telephone. In addition to this, face-to-face interviews were conducted to interview the prosecutors.

There were limitations with regard to the interviews with the SAPS cyber-crime technicians. The researcher tried to build a trusting relationship with the participants. All the participants were informed, and asked to give notice about the time they would be ready to be interviewed. Only four of the cyber- crime technicians were accommodating and agreed to take part in the research. Others informed the researcher that they were very busy, and that it was unreasonable of the researcher to expect them to take part in the research.

The researcher, who is also a member of the SAPS Crime Intelligence Division, understood that the reason for the above problems was because of the secrecy standards and the sensitive nature of the intelligence environment. Moreover, they were uncertain about giving out information through research, which could also be viewed as the leaking of information.

Despite the fact that the conducting of the research study was approved by the SAPS Crime Intelligence Division, the researcher tried for more than five months to persuade the participants in the research study to facilitate the revelation of the information. Also, the aim was not to force the participants, but to allow them to express their true feelings and opinions without fear. For this reason the researcher felt it would be unethical to do otherwise.

Limitations regard the interviews with the prosecutors, were as follows: The researcher aimed to interview five prosecutors – three from East London and two from Port Elizabeth. The aim of the researcher was to perceive the experiences of prosecutors regarding the seizing of computers in the investigation of cyber-crimes, by SAPS cyber-crime investigators. This could help to single out specific problems encountered when dealing with cyber-crime cases involving

computer seizure. There were few prosecutors trained to prosecute cyber-crimes: one in the East London area and four in Port Elizabeth.

The state prosecutors reported being very busy; nevertheless, three prosecutors took part. Their level of experience ranged from four years to ten years in the prosecution of cyber-crimes. One of them was a senior state advocate with eighteen years' experience in the field of prosecution in general.

According to Welman and Kruger (2001:158), guidelines for effective interviewing of participants has been studied. These were adhered to, including the way of developing and constructing interview schedules. The authors further explain some general rules and recommendations for interviewers, as follows:

- Dress in a way that will be more or less the same as the participants
- Be neutral, and not be seen as an intruder.

Kvale (1996:65) explains that the objectivity of the method used depends on its relationship to the nature of the object studied mainly, to clarify ambiguities and to follow up incomplete answers. The researcher documented or recorded on paper all the responses of the participants. Permission to conduct the interviews was obtained, and is attached as Annexure C, in order to comply with National Instruction 1/2006 of the SAPS (South African Police Service), which regulates requests to conduct research in the service, for the purpose of studies.

The interview schedules were perused by the supervisor to ensure that they were correct and measured what they were supposed to measure. According to Gratton and Jones (2004:18), to pre-pilot an interview schedule provides a useful run through for the interview, and may increase the researcher's confidence when it comes to the real interviews. The researcher did a pre-pilot of the interview schedules on two members who were not part of the sample. This was done before the actual interviews. The interview schedule for the prosecutors was checked by the supervisors, as it consisted of only a few questions. This means that the researcher used two different interview schedules to fit the two groups of participants.

The first group of participants consisted of SAPS cyber-crime technicians attached to the Cyber-crime Unit of the SAPS. Only four members were willing to participate in the research study. They all responded according to their knowledge and experience of cyber-crime investigations.

The positions of the SAPS participants were as follows: One participant was a constable with seven years' service, attached to the Cyber-crime Unit for more than four years. Another participant was a warrant officer with eighteen years' service, attached to the Cyber-crime Unit for nine years. The third participant was a lieutenant-colonel with thirty-two years' service, attached to the Cyber-crime Unit for twelve years. The fourth participant held the rank of colonel, with five years' service, attached to the Cyber-crime Unit for five years. Only three of the participants had received formal training in cyber-crime investigation. Their extent of dealing with the seizure of computers was 'not that much' and 'very much'. These answers were influenced by the levels of cyber-crimes in their provinces.

The second group of participants consisted of three prosecutors. The service of the prosecutors in the field of prosecution was as follows: One of the prosecutors had spent eight years as a prosecutor, and had prosecuted cyber-crimes for four years. Another prosecutor had spent thirteen years as a prosecutor, and had prosecuted cyber-crimes for eight years. The third prosecutor was a senior state advocate with eighteen years as a prosecutor, and had prosecuted cyber-crimes for ten years. They all prosecuted cyber-crimes on a regular basis, and had all received training in the prosecution of cyber-crimes.

1.11.3 Personal experience

The researcher is a member of the SAPS Crime Intelligence Division in East London. He has extensive experience in collecting digital computer evidence. He worked for more than 12 years as a technician in the Technical Support Services, a unit that resorts under the Crime Intelligence Division. The researcher was never a member of the Cyber-crime Unit, but he was, however, involved in the investigation of computer-related crimes. He qualified in electrical engineering, as a personal computer technician in computer networking, forensic auditing and computer

crimes.

1.12 DATA ANALYSIS

According to Hoyle, Harris and Judd (2002:245), data analysis assists and guides a researcher to detect patterns or problems, and to explore and determine if the data is consistent with the topic. Singleton and Straits (1999:455) comment that data analysis happens when theory and data are compared.

The researcher has studied Tesch's analysis process – an eight-step process for data analysis – and decided to make use of it to analyse the data for this research (Tesch, 1990:142-145). The researcher followed Tesch's analysis method to analyse the data obtained during this research project. This eight-step process for data analysis is as follows:

1	"Get a sense of the whole. Read through the transcriptions carefully and perhaps jot down some ideas as they come to mind.
2	Pick one document which could be the most interesting – the shortest or the one on top of the pile. Go through it, asking yourself: "What is this all about?" Do not think about the "substance" of the information, but rather its underlying meaning. Write down thoughts in the margin.
3	When you have completed the task of working through several documents, make a list of the topics that emerged. Cluster together similar topics, unique topics and leftovers.
4	Now take this list and go back to the data. Abbreviate the topics as codes, and write the codes next to the appropriate segments of the text. Try out this preliminary organising scheme to see whether new categories and codes emerge.
5	Find the most descriptive wording for your topics, and turn them into categories. Look at reducing your total list of categories by grouping topics that relate to each other. Perhaps draw lines between your categories to show the interrelationships.
6	Make a final decision on the abbreviation for each category, and alphabetise

	these codes.
7	Assemble the data material belonging to each category in one place, and perform preliminary analysis.
8	If necessary, recode your existing data.”

The researcher found the table of Tesch in line to analyse the data collected, and followed its steps. The researcher made use of a tape recorder during the interviews, to collect data. The researcher made sense of the collected data by listening to the recorded data, and wrote it down. The researcher then compared the data with the research topics. The purpose was to make substance of the data, according to the list of the research study topics. The data was then categorised according to descriptive wording of the topics. The researcher then started his analysis of the data.

1.13 METHODS TAKEN TO ENSURE VALIDITY

According to Denscombe (2002:100), validity is about the accuracy of the questions asked, the data collected, and the explanation offered. Validity relates to the data and the analysis used in the research study. Robson (2000:98) argues that validity is about measuring what one wants to measure.

The questions in the structured interview schedule were based on the research questions and aims of the research. This ensured that it measured what it was supposed to measure, and therefore ensured the validity of the data gathered. The use of more than one method to obtain data for this study, also known as triangulation (Mason, 1998:148), further enhanced the validity of the research. The use of Tesch’s analysis method to analyse the data, further ensured correct and proper analysis, and enhanced the validity of the research.

The researcher made use of a tape recorder to rewind each interview conducted. When he had finished conducting interviews, he listened to the tape and wrote everything down. He began to organise answers to each question asked. From the answers to each question, he found interrelationships for each category. Finally, he made findings, based on the responses of the

analysed information.

1.14 METHODS TAKEN TO ENSURE RELIABILITY

Singleton and Straits (1999:114) explain that reliability is concerned with the questions of stability and consistency. The pertinent question is whether the same results would be obtained if the research was repeated by another researcher. The structured interview schedule enhanced consistency, because the same questions were posed to all the participants. The interview schedule allowed participants to formulate their own responses, rather than being led or having suggestions put to them. The challenge that the researcher faced in this research, was the fact that some of the interviews were face-to-face, and others were over the telephone. The researcher strove to keep it consistent, so e-mail was used to forward the questions to the participants who were interviewed over the telephone. This ensured that the questions were clear, and in front of them, when the researcher interviewed them over the telephone. The structured interview schedule ensured that the same questions were posed to all the participants in the study, whether over the telephone or in person. The answers and responses to the questions were recorded on a tape recorder to ensure that all the information was captured properly.

1.15 ETHICAL CONSIDERATIONS

The researcher studied the guidelines on ethics in research, as explained by Leedy and Ormrod (2005:101), and adhered to them at all times. The guidelines are as follows:

- Protection from harm – there was no undue influence of whatever nature on the participants.
- Informed consent – there was voluntary participation of participants, and a clear understanding of the research study. The researcher obtained permission from the SAPS to conduct the research.
- Right to privacy – participants were not exposed to others, regarding the way in which they responded.
- Honesty with professional colleagues – researchers should be truthful about the findings, and not distort or mislead. Also, do not be ashamed to appraise or to give credit where it is due.

The researcher adhered to the codes as set out in the policies and procedures for postgraduate

studies in the University of South Africa Disciplinary Code for students, '(2007:3-4)', which stipulates that plagiarism is a form of theft of the work of others, and the work of the researcher must present the true results of the work claimed by the researcher. Also, as an employee of the SAPS, the researcher adhered to the 'SAPS (South African Police Service) National Instruction 1/2006', and applied for permission to conduct the research. The rights enshrined in the Constitution of the Republic of South Africa Act 108 of 1996, were adhered to. All participants were treated with dignity, and were allowed to participate voluntarily and remain anonymous and confidential.

1.16 CHAPTER OUTLAY

This chapter outlay summarizes the content discussed in each of the following chapters:

- **Chapter 2: The role of computers in facilitating the commissioning of crimes, in forensic investigation.**

This chapter dealt with the role of computers to make way for crimes to be committed, within the field of forensic investigation. At face value, the role of a computer would be typing, storing of information and communicating through e-mail. However, a computer also creates opportunities for people to engage in criminal activities. Hence, the following important aspects were covered in this chapter: the computer as a target, the computer as an instrumentality of crime, the computer as incidental to the crime, crimes associated with the prevalence of computers, malicious code and computer crime, investigation of computer crimes, and computer forensic investigation. Some aspects of this chapter extend over to Chapter 3, in order to cover the concepts of computer seizure as a process.

- **Chapter 3: Seizing computers without compromising evidence**

  The following aspects were discussed in this chapter: computer crime, computer forensics, computer evidence and its nature, types of computer data storage media, types of computer evidence, computer crime scene, seizing computer evidence, chain of custody, and legal aspects impacting on law enforcement of cyber-crimes.

- **Chapter 4: Findings and recommendations**

  This chapter reflects the findings and recommendations of the research, which are based on the information obtained from the literature and the interviews. Suggestions for further research are also included in this chapter.

CHAPTER 2

THE ROLE OF A COMPUTER TO FACILITATE THE COMMISSIONING OF CRIMES, IN FORENSIC INVESTIGATION

2.1 INTRODUCTION

It is important to understand that a computer is an electronic device which is capable of storing and processing information in accordance with a set of instructions (*South African Pocket Oxford Dictionary*, 2002:177). According to Swanson, Chamelin and Territo (2003:585), the first electronic computer was completed in 1945, and the first long-distance electronic communication was sent in 1969. The information society is structured today in a manner that depends entirely on computers and networks.

Brenner (2009) believes that the increase of computer technology and the development of the Internet have also created new opportunities for those who would engage in criminal or illegal activity. According to *Expert Law*, (2010), computers often contain important information which can be used as evidence in legal proceedings. This is the advent of computer forensics, which can be used to uncover potential evidence in many types of cases such as fraud, child pornography, corruption and money laundering. Mendell (2004:9) summarises the scope of computer crime as follows: physical crimes such as theft, burglary and terrorism, sexual exploitation, malicious e-mail and cyberspace frauds, alterations of programming code, malicious code viruses, penetrations of operating systems, manipulating input and output flaws, industrial spying, wiretapping and retail computer security.

According to *Computer Forensics World*, (2010), computer forensics can be of value in a wide variety of situations, including re-tracking steps taken when data has been lost. It is further explained that computer forensics relates to the application of analytical techniques employed to collect, recover, authenticate, preserve and analyse electronic data for legal purposes.

The purpose of this chapter is to inform the reader about the role of a computer in the act of crime and as evidence in forensic investigation. The following important aspects will be discussed in this chapter: the computer as a target, the computer as the instrumentality of crime, the computer as incidental to the crime, crimes associated with the prevalence of computers, malicious code and computer crime, investigation of computer crimes, and computer forensic investigation.

2.2 THE COMPUTER AS A TARGET

Swanson et al. (2003:589) explain that the computer is defined as "the target when an act effectively prevents the legitimate user or owner from receiving the service or data that he or she expects". *Ezine@rticles,* (2010) describes crime in which the computer is the target, as crimes such as theft of intellectual property, theft of marketing information (for example, customer lists, pricing data or marketing plans), or blackmail based on information gained from computerized files (for example, medical information and personal history). *Computer Crime*, (2010) agrees with *Computer Crime Research Centre*, (2005), in that these are crimes which could also entail sabotage of intellectual property, marketing, pricing or personal data, or sabotage of operating systems and programs with the intent to impede a business or create chaos in business operations. From his experience, the researcher agrees with the authors on the types of crime in which the computer is the target.

The four SAPS cyber-crime technician participants were asked about the role of a computer in forensic investigation. Three participants believed that a computer could be used as a tool to commit a crime, and that it could also be the target of a crime. One participant found it difficult to understand the term 'forensic investigation'. However, the researcher explained the term to the participant. The participant understood, and responded by saying that a computer could be used to commit a crime and it could also be the victim of a crime. It seems as if the participants were familiar with the important role of computers in the investigation of crime. Computers and networks could be targets of crime, used as tools in the commission of crime, and could be incidental to a crime. The researcher believes that the role of computers in investigation is on the increase as criminals become more technologically advanced.

Swanson et al. (2003:589) support the view that crimes, in which the computer is the target, incorporate the dismissal of envisaged service and the change of data. The following are some examples of these crimes and their negative impact on legitimate users or owners:

2.2.1 Computer manipulation crimes

Viridis, (2000) is supported by *Answerbag*, (2010) and Swanson et al. (2003:589), that computer manipulation crimes refer to the illegal use of a computer to conduct criminal activity, which involves changing data or creating electronic records to commit fraud or embezzlement.

2.2.2 Data alteration or denial

According to *Computer Crime*, (2010), "data alteration is a crime which has been constantly affecting many people as it targets the computer directly by attacking information stored in the computer".

2.2.3 Hacking and other forms of network intrusion

Hacker (*Computer Security*), (2010) points out that "hacking and other forms of network intrusion are a kind of unauthorised use or penetration of a wireless network which involves simply breaking the encryption". Swanson et al. (2003:591) point out that hacking or cracking is a process of gaining unauthorized entry into a computer system.

2.2.4 Denial of service

"Denial of service is an attempt to make a computer service unavailable to its intended users" (*Denial-of-Service Attack*, 2010). Swanson et al. (2003:593) argue that service denial is more direct, and it has a very negative effect on the users as it makes services unavailable.

2.2.5 Computer vandalism

Your Computer Dictionary, (2010) explains that "computer vandalism is a program that performs malicious function such as extracting a user's password or other data or erasing the hard disk".

2.3 COMPUTER AS AN INSTRUMENTALITY OF CRIME

In an attempt to assess the role of the computer as an instrument to commit crime, the following authors detail some methods and activities which take place in the commission of such offenses:

- Swanson et al. (2003:593) find evidence that in "computer-as-instrumentality crimes, the perpetrator only uses the computer to advance a criminal end". This means that the computer and the data contained therein are not the article of the crime.
- Bologna (1989:10) points out that there are computer crimes which involve the computer as a means or instrument for initiating the crime – for example, when the computer is used to commit fraud and embezzlement. He states that these are the most reported crimes in cases where there is submission of false and fraudulent vendor invoices, expense claims, salary claims and benefit claims for payment.
- *Brenner*, (2009) demonstrates that there is a possibility of committing homicide by hacking into the computer system of a hospital – for example, by altering the records establishing the type and dosage of medication a patient is to receive, so that the patient actually receives a lethal dose of medication. The author comments that the offence committed is a traditional one; however, it is committed by a perpetrator who may be hundreds or even thousands of miles away from the victim at the time the death occurred. In this scenario, the computer is simply a tool used to commit a traditional crime.
- The researcher agrees that a computer does not only replace pen and paper, but that people adapt technology for various uses. The researcher is of the opinion that these crimes threaten the security of information and communications systems. The computer is a valuable device which is a nucleus of communication systems worldwide. However, the role of a computer to facilitate the commissioning of crime is difficult to comprehend.

2.4 THE COMPUTER AS INCIDENTAL TO THE CRIME

According to Swanson et al. (2003:598), this is a class where the computer does not guide the illegal transaction, but assists it in producing an intended result. This view is supported by the following sources from the Internet: *Ezine@rticles,* (2010) supports the view that when a computer is incidental to crime, it is a category in which it is not essential for the crime to occur, but is related to the criminal act. Some examples of these crimes include money laundering,

criminal enterprise, processing of pornographic information, unlawful banking transactions, and erasing data files. *NTI*, (2010) agrees with Swanson et al. (2003:598), that in this category of computer crime, the computer is not essential for the crime to occur. However, the computer systems facilitate the offences – for example, by helping the computer crime to occur faster by processing of greater amounts of information, by making the computer crime more difficult to identify and trace, and so on.

Computer crime, (2010) explains that it means that these crimes could occur without the use of technology; however, computerisation helps to speed up the commission of the crime. For example, in the case of child pornography, consumers of child pornography traffick photographs and related information through newsletters and tightly controlled exchange networks. The advancement of computer technology enables child pornographers to exchange this information through bulletin board systems. This Oxford is a site on a computer where any user can read or write messages (*South African Pocket Dictionary*, 2002:110).

Carter (2010) believes that these criminals use the computer to facilitate the distribution of pornographic material and increase the efficiency of criminal activity by using computers. Swanson et al. (2003:599) point out that in September 1998, over 200 people were arrested in 21 countries during the largest child pornography sting operation. They comment that more than 100 000 indecent images of children were confiscated in the United States, Australia and Europe. Most importantly, these images were being traded among child pornographers over the Internet. This implies that a computer was used for ease in maintaining the efficacy of the crime, as pointed out by Swanson et al. (2003:598).

2.5 CRIMES ASSOCIATED WITH THE PREVALENCE OF COMPUTERS

According to *Articlesbase*, (2010), crimes associated with the prevalence of computers provide law enforcement with an insight for investigative strategies. *Technology and lifestyles*, (2010) comments that the presence of computers and microcomputers generates disturbing changes in traditional crimes such as software piracy, counterfeiting, and copyright violation. These crimes result in the loss to businesses. According to *Cyber-crime Investigation Cell*, (2010), illegal

software helps hackers to break into computers. Illegal sales of successfully duplicated computer programs, and pirated items such as modems and hard disks, are crimes associated with the prevalence of computers.

Computer Crime, (2010) states that discussions on emerging technological crimes centre mostly on computer crimes with specific categories. For this reason, an increasing need emerges for police personnel in general to understand how crimes associated with the prevalence of computers vary. However, *Cyber-crime Investigation Cell,* (2010) points out that these crimes can occur during any given criminal transaction, resulting in an overlap between the transactions. *Computer Crime,* (2010) alerts one to the fact that one offence in crimes associated with the prevalence of computers, occurs with relative frequency: the violation of copyright restrictions of commercial software. This results in crimes such as theft of intellectual property or theft of information.

Swanson et al. (2003:600) and *Computer Crime,* (2010) state that computer crime investigators should be mindful of new targets of crime. For this reason it is imperative that certain crimes and terminology associated with these crimes be clarified here. According to these two authors, crimes that are associated with the prevalence of computers are the following:

2.5.1 Intellectual property violations

Intellectual property violations are set out as piracy. Large-scale piracy exists worldwide. These activities include software piracy and music piracy. From the researcher's experience, this is done by copying or selling the product without the copyright. For that reason, those who worked to produce the product do not receive the money for the work they have done.

2.5.2 Misuse of telephone systems

This is a crime carried out by people who trick telephone systems into accepting long-distance service and airtime as being legitimate. In addition to this is the cloning of cellular phones by using a personal computer. They change the microchips in one cellular phone so that it tones with legitimate mobile identification and electronic serial numbers hacked from a phone

company.

2.5.3 Component theft

This is the theft of equipment such as desktop and laptop computers, monitors, printers, scanners and modems.

2.5.4 Corporate Crime

This is viewed as part of doing business, as the doubtful practices comprise rebate fraud. Rebate fraud occurs when there is a promise in an advertisement about a partial refund to someone, when it's not true, while simple fraud may be as a result of bankruptcy of the company which will take new orders and not fulfill the deals with customers.

2.6 MALICIOUS CODE AND COMPUTER CRIME

Malicious code and computer crime mainly refers to the types of tools that can be used to commit crime – with which investigators should be acquainted. These tools can be discovery tools, cryptanalysis software, exploits and attack codes (Swanson et al., 2003:604). The authors comment that being in possession of such tools does not amount to crime, unless there is evidence of their use. For example, a crime can be committed by linking compiled computer programmes to an original source, and matching test-based commands and comments to gain illegal access to the computer system. *Freedom From Fear Magazine*, (2010) supports the view about the use of malicious code to exploit a computer system's vulnerabilities. They explain that malicious code is used to create crimeware viruses such as Trojan horse and Key Loggers, to gain flexibility of controlling, stealing and trading data.

2.6.1 Discovery tools

Swanson et al. (2003:604) explain that discovery tools attack targets' vulnerable systems. These discovery tools are categorised as port scanners, war dialer and sniffer tools. The following is a brief discussion of these tools:

2.6.1.1 Port scanners

Port scanners contain descriptions for common ports, and can perform scans on predefined port

ranges (Radmin, 2010). According to *Port Scanner*, (2010), a port scanner is a software application designed to probe a server or host for open ports. Such attacks are aimed at finding an active port and exploiting a known vulnerability of that service. Swanson et al. (2003:604) comment that should the vulnerabilities of that system be known, exploiting that vulnerability is as simple as entering the Internet address in an exploit programme.

2.6.1.2 War dialer

War dialer, (2010) defines a war dialer as "a technique that uses a modem to automatically scan a list of telephone numbers to search for computers, bulletin board systems and fax machines". This is done by dialing the number which will be copied by the war dialer to gain access within the computer when replied to. *Search Security* (2010) supports the view that a war dialer is used to identify the phone numbers that can successfully make a connection with a computer modem. When a successful connection to the modem is made, some programs, and the type of operating system, are identified, and also, user names and passwords found are used to gain access to the system.

2.6.1.3 Sniffer

Sniffer, (2010) describes a sniffer as "a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network". *Sniffer*, (2010) further states that data streams flow across the network and then the sniffer captures each packet and, if needed, decodes and analyses its content according to the appropriate specifications.

2.6.2 Cryptanalysis software

Webopedia Computer Dictionary, (2010) describes cryptanalysis as "the study of a cryptographic system for the purpose of finding weaknesses in the system and breaking the code used to encrypt the data without knowing the code key".

2.6.3 The use of exploits

Exploits are programs designed to profit by a security hole or back door, to sidestep normal security procedures (Swanson et al., 2003:604). *Computer Exploits*, (2010) supports the view that an exploit is a prepared application that takes advantage of a known weakness. In addition to this, a special exploit package known as 'root kits' enables the intruder to maintain the level

of access by installing back doors and secret accounts, and by changing logs and basic system services (Swanson et al., 2003:605).

2.6.4 Attack codes

Swanson et al. (2003:605) describe an attack code as "malicious software intended to impair or destroy the task of another computer or network resource". These intrusion aids are designed for harassing users of the system. The following is a brief discussion of some of these codes:

2.6.4.1 Denial-of-service attacks

Search Software Quality (2010) defines a denial of service attack as "an incident in which a user or organisation is deprived of the services of a resource they would normally expect to have". This view is supported by *National Cyber Alert System*, (2010), which acknowledges that an attacker attempts to prevent legitimate users from accessing information or services.

Attack Codes, (2010) explains that an attempt to make a computer resource unavailable consists of concerted efforts from a person to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. One common method of attack involves saturating the target machine with external communication requests, so that it cannot react to valid traffic, or reacts very slowly so as to cause it to be effectively unavailable. Swanson et al. (2003:605) find evidence that the tools used were developed for the purpose of irritating users, as their use constitutes a denial of service attack.

2.6.4.2 Logic bombs

Kabay (2008:1) defines a logic bomb as "a program delivered when a particular logical condition occurs". *Search Security*, (2010) describes a logic bomb as a programming code inserted intentionally to corrupt or even delete data, or to have other undesirable effects. *Logic Bombs*, (2010) urges that "a logic bomb is a piece of code intentionally installed into a software system that will set off a malicious function when specified conditions are met". Swanson et al. (2003:606) state that a logic bomb is a malicious program aimed at misusing legitimate instructions to spoil data structures.

2.6.5 Delivery vehicles to supply offensive software

Delivery vehicles are tools which serve computer criminals with a means of supplying their offensive software (Swanson et al., 2003:607). Discussed below are the most common types of delivery vehicles:

2.6.5.1 Trojan horse

Kabay (2008:3) explains that a Trojan horse is an innocent looking program that has undocumented and criminal functions. For example, it can change data in a particular way, record passwords for later inspection, send confidential information to unauthorized destinations, or are back doors into compromised systems. *Norton*, (2010) describes a Trojan horse as "files that claim to be something desirable but are, in fact, malicious, and cause loss or even theft of data". *Trojan horse*, (2010) supports the view that these files seem to perform an attractive use for the user prior to 'run' or 'install'. However, they allow unauthorised access to the user's computer system; therefore, this is a dangerous piece of software that works legitimately while users are tricked into loading and executing it on their systems (*Cisco*, 2010).

Trojan horse, (2010) caution that this is a program that may modify the user's computer to show advertisements in unwanted places – for example, on a user's desktop. In addition to this, Trojan horses may allow a hacker remote access to a target computer system (*Norton*, 2010). *Norton* (2010) further explains that once a Trojan horse has been installed on a target computer system, a hacker may gain entry to the computer remotely and carry out different operations, depending on the privileges of the user on the target computer system and the design of the Trojan horse.

Trojan horse, (2010) explains a number of methods in which a Trojan horse can be installed: software downloads, bundling, e-mail attachments, websites containing executable content, and application exploits. When a Trojan horse has been installed in a computer system, it becomes difficult to realise the extent of damage done and what other problems have been introduced. *Trojan horse*, (2010) advises users to simply erase all data from the hard disk, and reinstall the operating system and required software.

Groth and Skandier (2005:486) and *Beginner*, (2010) point out that a Trojan is a malicious process that can possibly be trusted, that users execute without knowing it, and as something one may think is safe, but hidden inside is usually something harmful. The authors further comment that the lure of a Trojan horse is that one may download a game or a picture, thinking it's harmless, but it will cause damage to one's system. Swanson et al. (2003:608) point out that a Trojan horse pretends to be a legitimate program which could be accepted by the computer user.

2.6.5.2 Viruses

According to *Beginner*,(2010), "a virus is a computer program with the sole purpose of destroying data on computers" – for example, by causing an infected computer to perform strange things on certain dates, as well as issuing serious commands such as erasing registry files – thus disabling the operation and booting up of computers. Kabay (2008:3) explains that a virus can infect executable code in programs – for example, Execute and command files under DOS, boot sectors on disks, and macro programs. *Norton*, (2010) agrees with Kabay (2008:4), in that file infector viruses infect program files such as command and execute files. *Norton,* (2010) agrees with Kabay (2008:4), that a file infector virus infects program files such as command and executes files.

Norton, (2010) points out that there are five recognized types of viruses:

- Infector viruses – these are viruses that infect program files.
- Boot sector viruses – these viruses infect the system area of a computer record on floppy disks and hard disks.
- Master boot viruses – these viruses are memory – residential in the same manner as boot sector viruses.
- Multipartite- these are viruses which are boot sector and program files.
- Macro viruses – these types of viruses infect data files.

O'Brien and Marakas (2009:627) explain further that a virus is a self-replicating program that opens out by placing copies of itself into other executable code or documents. This view supports Swanson et al. (2003:608), who mention that the computer virus is not active without a host, because a computer virus attaches to a host by inserting instructions within the program.

2.6.5.3 Worms

According to Swanson et al. (2003:608), worms do not rely on contaminating a host program. For that reason, worms are programmed to work faster even before antivirus software can be brought up to date. *Norton,* (2010) agrees with Swanson et al. (2003:608) that worms replicate themselves from system to system, without the use of a host program to allow them to spread and

infect host files. Kabay (2008:3) supports the view of Swanson et al. (2003:608), in that a worm is a program which spreads through a computer system or network by replicating, without merging itself into other executable code.

2.6.5.4 Hacker

The (*South African Pocket Oxford Dictionary,* 2002:402) is supported by Wikipedia the free encyclopedia (2010) in that "a hacker is a person making use of a computer to gain unauthorised access to data". Swanson et al. (2003:610) explain that the hacker's best weapon is a fast computer with large hard disk, a modem, and a telephone line in order to access information.

Kabay (2008:4) is of the opinion that the term 'hacking' has been used synonymously with the term 'cracking', due to ignorance of under-educated journalists. The term 'hacking' originally meant efforts made that involved intense study, dedicated analysis, and learning about the technical field, including computing. This view is supported by *Hacker* (*Computer Security*), (2010), which states that before the media described the person who breaks into computers as a hacker, there was a hacker community. *Hacker* (*Computer Security*), (2010) points out that students who did computer programming and computer science, referred to themselves as hackers because they were able to take programs and have them perform actions not meant for the program. However, the meaning does not change the use of the terms 'hacking' and 'cracking' as synonymous. Fortunately, the authors also acknowledge that it is probably too late to reverse the shift in the meaning.

Swanson et al. (2003:612) believe that hackers are not socializing people. Rather, they make use of their computers to communicate with their peers. *Hacker* (*Computer Security*), (2010) states that hackers have different attitudes and aims, making use of different terminology to demarcate themselves from one another, or even try to keep out specific groups where they don't agree. *Hacker (Computer Security*), (2010) finds evidence that these subgroups might be defined by the legal status of their activities as follows:

2.6.5.4.1 White hat hacker

> This is the kind of hacker who breaks security for non-malicious causes. In this classification, individuals who perform penetration tests and vulnerability assessments

within a contractual agreement, also fall under this categorisation.

2.6.5.4.2 Grey hat hacker

A black hat combines with a white hat to produce a grey hat, which moves from site to site on a computer system, for the sole purpose of notifying the administrator of the hacked system and offering to repair it for a small amount of money.

2.6.5.4.3 Blue hat hacker

This is a hacker outside computer security consulting firms, who is used to bug or test a system prior its launch, looking for exploits so that they can be closed. For example, Microsoft also uses the term 'blue hat' to represent a series of security briefing events.

2.6.5.4.4 Black hat hacker

This is a person who is also referred to as a ‘cracker’, because they break computer security without authorisation, or make use of technology such as a computer, phone system or network, for vandalism, credit card fraud, identity theft, piracy, or any illegal action.

2.6.5.4.5 Hactivism

A hacktivist is a hacker who uses technology to announce a social, ideological, religious or political message. In general, most of it entails website defacement or denial-of-service attacks, and is used as a tool for cyber terrorism in extreme conditions.

2.6.5.5 Cracker

According to Casey (2000:171), cracking is a kind of computer attack perpetuated through the Internet on the connections of the organisation’s systems. O’Brien and Marakas (2009:524) describe a cracker “as malicious of criminal hacker”. The authors further explain that is a person who benefits through the knowledge of the vulnerabilities of computers and exploits them for private advantage, and will never reveal them to anyone. Casey (2000:11) is supported by O’Brien and Marakas (2009:524), in that the term ‘cracker’ has been used by the media and the general public to mean the same thing as ‘hacker’. However, these are two different entities making use of computers for different reasons. Nevertheless, it is very important to find out how these crimes are investigated. This issue is exploited in the next section.

2.7 INVESTIGATION OF COMPUTER CRIMES

Cross (2008:202) is of the view that one fears things that one does not understand. It may be the reason why many investigators shy away at the mention of a computer-related crime. It is important for investigators to realize that computers are yet another source of evidence, and that they must learn how to investigate crimes where a computer is involved. Cross (2008:202) explains further that it is important for investigators to keep up with new technology, in order to be effective in their investigations. It does not mean that all investigators must become experts, but there are basic concepts and methods that an investigator should learn, so as to put them ahead of the average computer user. These skills will enable them to apply investigation procedures to computer-related crimes.

2.7.1 Investigation as a process

Swanson et al. (2003:glossary page 11) define investigation as a process of establishing that a crime was committed, identifying and apprehending the suspect, recovering the stolen property, if any, and assisting in the prosecution of the person charged with the crime. According to Marais and Van Rooyen (1990:17), investigation of crime is "a scientific and systematic search for the truth with the purpose of clearing up the committed crime". Cross (2008:205) points out that an investigation starts with a crime being committed and someone noticing it. Cross (2008:210) further explains that investigation methodology refers to "the practices, procedures, and techniques used to collect, store, analyse and present information and evidence that is obtained through a computer forensic investigation". The researcher agrees with Cross, that a logical investigation process needs to be followed to ensure that the evidence is accepted in a court of law.

2.7.2 Objectives of investigation

From the definition of investigation given by Swanson et al. (2003:11) and Marais and Van Rooyen (1990:17), the researcher deduces and believes that the objectives of investigation are to ascertain the truth of any alleged matter under investigation. For this reason, the ability to analyse, collect and use evidence determines the degree of success of the investigators. In addition to this, *Longman's South African School Dictionary,* (2009:373) defines investigation as "an official attempt to find out about something, especially of crime or incident". The *South African Pocket Oxford Dictionary*, explains the term 'investigate' as "to carry out a systematic enquiry into an incident or allegation so as to establish the truth". One can conclude by saying that the objectives of investigation are to determine the circumstances contributing to the exposure of the event, and to evaluate the effectiveness of the law regulating the offence.

Cross (2008:680) and Mendell (2004:5) list the objectives of investigation as follows:

- Determine whether a crime has been committed.
- Establish the facts that constitute a crime.
- Protect the crime scene.
- Preserve the evidence.
- Determine the leads available to find suspects.
- Use and supervise experts as needed.
- Identify the suspect(s).
- Identify the modus operandi (method of operation).
- Prove that the suspect(s) did it.
- Apprehend the suspect(s) and prepare for prosecution.

The four SAPS cyber-crime technician participants were asked what the objectives of forensic investigation are. They were very brief, but their answers were in line with the literature. One of the four participants said they were to find evidence, to determine clues to find offenders and to preserve evidence for the judgment of the court of law. The other participants said that the objectives were to arrest the suspect. The other two participants believed that it is to establish the truth about the alleged offence.

The researcher agrees with the four participants, based on his work experience. This is also in line with the literature. For example, Swanson et al. (2003:11) and Marais and Van Rooyen (1990:17) state that the objectives are to ascertain the truth of any alleged matter under investigation. In addition to this, Cross (2008:680) and Mendell (2004:5) table the objectives in a more detailed form, as shown in the previous paragraph.

Cross (2008:680) further believes that when the following questions have been answered the next step is to effect a lawful arrest of the suspect:

- What happened?
- Who was involved?
- Where did the illegal act occur?

- When did it happen?
- Who had motive, means and opportunity?
- How was the act committed?
- Who observed the crime or its results?
- Where was the suspect when the crime occurred?
- What records/documents/logs identify the suspect?
- Why did it occur?

The researcher is familiar with all these questions – known as the 5WH approach. These questions assist an investigator to achieve the objectives of an investigation. *Ezine@rticles*, (2010) explains that the 5WH questions formula applies to every business decision to be made. This approach was also the view of Bologna (1989:6) to determine when, where, how and by who was fraud likely to be committed and why it occurred.

2.7.3 Phases of investigation

Gilbert (2004:64) explains that the investigation of crime is made up of three phases, as follows:

- Preliminary investigation – is a stage where a crime has been reported, the crime scene has to be managed properly and evidence gathered from the crime scene.
- In-depth investigation – is the stage where witness statements are obtained, forensic reports are made available, and the suspects are identified.
- Final investigation – involves the arrest of the perpetrator(s) and taking the case docket for a court decision.

According to Cross (2008:210), a computer forensic investigation consists of three basic phases, as follows:

- Acquisition – the gathering of information and evidence.
- Authentication-ensuring that the acquired evidence is the same as the data that was originally seized.
- Analysis-examining and evaluating the information.

The SAPS cyber-crime technician participants were asked what the phases of computer investigation are. The term 'phases' was not clear to all the participants. Two of the participants indicated that they did not know what the phases of computer investigation are. The other two participants said the phases are the stages taken to carry out the investigation process.
It is clear to the researcher that this is due to a lack of proper training in computer investigations. This implies that training manuals used do not cover all critical aspects necessary to gain enough knowledge in the investigation process. The phases are necessary to protect and preserve the evidence during the recovery process, so that it can be admissible in a court of law. If the participants are not familiar with all the phases, there is the potential of failure to maintain the chain of custody of the evidence seized.

According to Fisher (2004:1), evidence can be divided into two extensive forms: real or physical evidence, and testimonial evidence. 'Tshwane University of Technology (2002:50)' see (P96), is supported by the findings of Fisher (2004:1) about the types of evidence. Tshwane University of Technology (2002:50) further explains that physical evidence is any evidence that has an objective existence with size, shape and dimension, while testimonial evidence is based on personal opinions or feelings of individuals. Cross (2008:675) explains that the law generally recognizes three different types of evidence: physical evidence that is tangible items – for example, a knife that was used to commit a crime; direct evidence – the testimony of a witness who saw the crime occur, or observed the accused taking steps towards committing a crime, or has direct knowledge of the crime; and, circumstantial evidence, which consists of facts and circumstances that may support the theory that the suspect committed a crime, but does not offer direct proof. Cross (2008:676) further states that in cybercrime cases, much of the evidence is digital – which means that it is not tangible evidence. It is made up of electronic or magnetic pulses that are stored in the form of electromagnetic charges on a disk or tape. It is very fragile and can be compared to a footprint in the snow; it must therefore be captured before it melts away. The nature and processing of computer evidence is dealt with in detail in Chapter 3 of this research dissertation.

2.8 Computer Forensic Investigation

Cross (2008:202) explains that the term "forensics" is a Latin word for a forum, in which legal disputes were settled in ancient Rome, but in today's world this term is applied differently. The author points out that, as with other areas of forensics, "computer forensics refers to an investigation process of gathering and examining evidence to establish facts so that accurate testimony and evidence can later be presented in court or other hearings". Casey (2004:20) states that 'forensic' can mean "a characteristic of evidence that satisfies its suitability for admission as fact and its ability to be persuaded based upon proof or high statistical confidence". Basically, forensic science is the application of science to the law. *Chunovic*, (2008) explains that a forensic investigation is the technique of examining how an event occurred. He further explains that a forensic investigation might point to the different levels of conclusions, based on the investigation.

The SAPS cyber-crime technicians participants were asked what forensic investigation is. Two of the participants believed that forensic investigation has to do with the use of technology. Another participant said it had to do with the investigation of computers. The fourth participant said it had to do with scientific methods in the investigation of crime.

Although none of the participants could provide an accurate definition of the term as stated in the literature, the researcher is of the view that they did understand what it entails. From their answers it is clear that they understood that technology and science play a role in the forensic investigation process.

Computer Forensics, (2010) describes computer forensics as "a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media". *Intratec Data Recovery*, (2010) describes computer forensics "as the preservation, identification, extraction, interpolitation, analysis and documentation of computer evidence". Casey (2002:195) and *Intratec Data Recovery,* (2010) mentions that such evidence is used as evidentiary material in a court of law. Vacca (2002:3) is also of the view that computer forensics is about collecting evidence from computers, and that it should be sufficient to make its way in court and be

persuasive. The author further explains that it entails aspects such as analysis, electronics evidence discovery, data recovery and examination of both computers and media such as hard disks and diskettes, for evidence.

Marais and Van Rooyen (1992:1) states that “criminal or crime investigation can be regarded as a process of identification of people and physical objects from the time the crime is committed until the guilt of the perpetrator is either proven or disproven in court”. For that reason there is no real difference between forensic investigation and criminal or crime investigation, as the terms are used interchangeably by different people. For example, the private sector refers to their investigation units as forensic investigation units, while SAPS members refer to their investigations as criminal or crime investigations. The term 'forensic investigation', according to the researcher’s observation, has become very popular because of television programmes. The media, therefore, mostly refer to all investigations by the SAPS as criminal investigation, and private industry investigations as forensic investigations. The four SAPS cyber-crime technician participants were asked if there is any difference between forensic investigation and criminal investigation, and if the answer was 'yes', they had to explain the difference.

The participants all answered 'yes' and explained the difference between the two concepts as follows: One of the four participants said forensic investigation is based on scientific evidence, while criminal investigations are based on traditional crimes such as murder, theft and fraud. Another participant explained that forensic investigation is the use of technology, but criminal investigation deals with crimes that could be investigated by taking statements from victims of crime, eyewitnesses and suspects. Two other participants believed that criminal investigations refer to investigation methods applied in the olden days and are still applicable to date; however, forensic investigations refer to modern methods of investigation with the application of science, to reveal the truth.

The researcher learnt that these terms are used interchangeably by different people in different fields of investigation. In a nutshell, there is no real difference, as the measures taken are used to identify offenders, and to prove or disprove guilt in a court of law, irrespective of the era.

However, a forensic investigation can also include a civil investigation, while a criminal investigation only refers to criminal matters.

2.8.2 Types of data associated with computer crime

The researcher has established, through the literature search, the need to understand the types of data to determine actions surrounding a criminal activity. Data is essential in the reconstruction of an event. Fisher (2004:193) emphasises that computer data must be attended to like any other seized evidence. This will always help investigators to understand what happened. The researcher also experienced that looking for supporting physical evidence adds value to interpret data recovered – for example, computer peripherals.

The four SAPS cyber-crime technician participants were asked what the types of evidence pertaining to computer data are. One of the participants mentioned documents, data and e-mails. The other participant mentioned documents, e-mails, and data on CDs and hard drives. The third participant mentioned data stored in the computer and its peripherals. The fourth participant mentioned data on floppy disks, CDs, memory sticks and memory cards, DVDs, and USB devices.

The researcher believes that the participants understood some of the items that should be seized for the retrieval of data, which would amount to computer evidence.

According to *The Computer Forensic Examination Process*, (2012) and *Intratec Data Recovery*, (2010), there are three types of data which are of concern in computer forensic investigation. These are active data, archival data and latent data, which are described as follows:

2.8.1.1 Active data

Active data is information that can be seen by the naked eye –for example, data files, programs, and operating systems.

2.8.1.2 Archival data

Archival data is that data which has been backed up and stored –for example, floppies and hard drives.

2.8.1.3 Latent data

Latent data is the data or information that requires special tools to deal with – for example, this may be information that has been deleted or partially overwritten.

2.8.2 Types of computer crimes and the nature of evidence

There are crimes and evidence which are unique to a computer. Therefore, it is an issue of paramount importance to provide examples of such crimes and where evidence can be located. *United States Secret Service*, (2010), *Intratec Data Recovery*, (2010), and *The Computer Forensic Examination*, (2012) point out the types of crimes and the type of evidence that may be recovered during forensic investigations, as follows:

2.8.1.4 Computer fraud investigations

Swanson et al. (2003:597) explain that computer fraud exploits the trust guaranteed by law in business transactions. Computer fraud investigation can be carried out by looking at the following: account data from online auctions; accounting software and files; address books; calendars; chat logs; customer information; credit card data; databases; digital camera software; e-mail, notes and letters; and financial and asset records.

2.8.1.5 Child abuse and pornography investigations

According to Swanson et al. (2003: 599) the Internet is used for tempting unsuspecting children to pedophiles and for distributing child pornography. *United States Secret Service*,(2010) explains that to investigate child abuse and pornography, evidence can be found from chat logs; digital camera software; e-mails notes and letters; games; graphic editing and viewing software; images; Internet activities logs; movie files; user created directories; and, file names which classify images.

2.8.1.6 Network intrusion investigations

Fisher (2003:193) explains that when one encounters a computer or any type of computer peripherals or data at a crime scene it is important not hurry. *The Computer Forensic*

Examination Process, (2012) states that evidence can be found on the following: address books; configuration files; e-mails, notes and letters; executable programs; Internet activity logs; internet protocol address and user names; internet relay chat logs; and, source code: text files and documents with usernames and passwords.

2.8.1.7 Homicide investigations

Bologna (1989:1) believes that forensic auditing skills can be useful to determine the financial motive, to analyse financial clues and to identify possible payments on a contract for homicide. To investigate homicide, evidence can be found on the following: address books; e-mails, notes and letters; financial asset records; Internet activity logs; legal documents and wills; medical records; telephone records; diaries; maps; and, photos of the victim(s) or suspect(s) trophy photos (*United States Secret Service*, 2010).

2.8.1.8 Domestic violence investigations

Swanson et al. (2003:324) believe that domestic violence is underreported because people are ashamed and afraid of reprisal if they speak out. According to *United States Secret Service*, (2010), the following are important to look for in domestic violence evidence: address books; diaries; e-mails, notes and letters; financial asset records; and, the telephone.

2.8.1.9 Financial fraud and counterfeiting investigations

O'Brien and Marakas (2009:525) explain that computer crimes involve theft of money through unauthorized network entry and fraudulent alteration of computer databases. According to *United States Secrete Service*, (2010) the following are very important for investigation of financial fraud and counterfeiting: address books; calendars; currency images; check and money order images; customer information; data bases; e-mails, notes and letters; false identification; financial asset records; images of signatures; Internet activity logs; on-line banking software; counterfeit currency images; and, bank logs and credit card numbers.

2.8.2.1 E-mail threats, harassment and stalking investigations

Cyberstalkers are able to threaten victims more immediately than physical stalking (Swanson et

al. 2003:598). *Intratec Data Recovery*, (2010) explains that evidence can be found on the following during forensic investigations: address books; diaries; e-mails, notes and letters; financial asset records; images; Internet activity logs; legal documents; telephone records; victim background research; and, maps to victim locations.

2.8.2.2 Narcotics Investigations

Fisher (2004:311) states that police commonly encounter various types of drugs and examine them. Evidence can be found on the following: address books; calendars; databases; drug receipts; e-mails, notes and letters; false id; financial asset records; Internet activity logs; and, prescription from images (*United States Secret Service*, 2010).

2.8.2.3 Software piracy investigations

According to Swanson et al. (2003:600) software piracy constitutes intellectual-property violations. The *Intratec Data Recovery*,(2010) explains that evidence can be found on the following: chat logs; e-mails, notes and letters; image files and software certificates; Internet activity logs; software serial numbers; software cracking utilities; user created directories and file names which classify copyrighted software.

2.8.2.4 Telecommunication fraud investigations

Swanson et al. (2003:601) state that telecommunication fraud involve tricking telephone systems and cloning of cellular phones by hackers. Evidence can be found on the following: cloning software; customer database records; electronic serial numbers; mobile identification numbers; e-mails, notes and letters; financial asset records; and, Internet activity logs (*United States Secrete Service*, 2010).

2.8.2.5 Identity theft investigations

United States Secret Service, (2010) explains that evidence can be found on the following: hardware and software tools; Internet activity related to identity theft; identification templates;

and, negotiable instruments. Identity theft occurs when a person pretends to be someone else in order to trick people. The following are some aspects to look at for evidence during a forensic investigation:

- Hardware and Software tools
  - Backdrops
  - Credit card reader or writer
  - Digital camera software
  - Scanner software
- Internet activity related to identity theft
  - E-mail and news group postings
  - Deleted documents
  - Online orders
  - Online trading information
  - Internet activity logs
- Identification templates:
  - Birth certificates
  - Cheque cashing cards
  - Digital photo images
  - Driver's licenses
  - Electronic signatures
  - Counterfeit vehicle registrations
  - Counterfeit insurance documents
  - Social security cards
- Negotiable instruments
  - Business checks
  - Cashier's checks
  - Credit card numbers
  - Counterfeit court documents
  - Counterfeit gift certificates
  - Counterfeit loan documents

- Counterfeit sales receipts
- Money orders
- Personal checks

The SAPS cyber-crime technician participants were asked about the types of crimes associated with computers. One of the participants mentioned child pornography, fraud and theft. The other participant mentioned fraud, pornography, theft of information and money laundering. The third participant mentioned fraud, theft of documents and information, pornography and piracy. The fourth participant mentioned fraud, theft of information, pornography and theft of information.

The researcher believes that the participants understand the crimes associated with computers. However the participants did not mention crimes such as homicide investigations, domestic violence investigations, e-mail threats, harassment and stalking investigations and narcotics investigations. The researcher agrees with the four participants on the types of crimes. Nevertheless, the discussion on the research study showed more detailed categories to be used as sources of computer crimes.

It is evident from the information above that important evidence can be obtained from a computer but that it first have to be identified in order to obtain it as evidence.

2.9 SUMMARY

The advancements in technology created new ways of committing crimes such as the use of computers. The research has revealed important types of cyber-crimes based on the role of computer in the commission of crime. The study demonstrates that a computer can be incidental to other crimes. It can also be associated with the way criminals have adapted the advancements of computer prevalence to further their own illegal activities, it can be a target of the crime and it can be used as an instrument to commit a crime.

The study also gives a brief, but sharp analysis of the criminal motive behind the use of a computer in different categories, including the tools and methods of committing crimes. This

study alerts us to the fact that computer technology and the development of the Internet has created new opportunities for people who would engage in criminal or illegal activities.

Ultimately the study informed the reader about the issues concerning and related to the role of a computer in forensic investigation. Above all, criminal actions can out-pace the ability of police to respond effectively if not noticed. Forensic investigation is the technique of examining how an event occurred. There is no real difference between forensic investigation and crime investigation, computer forensic is the method of investigating evidence found in computers.

The following chapter will focus on seizure of computers without destroying evidence.

CHAPTER 3

SEIZING COMPUTERS WITHOUT COMPROMISING EVIDENCE

3.1 INTRODUCTION

According to *Field Guide, Part Six,* (2011), seizing computers without compromising evidence is essential for the evidence to stand proof the case in the court of law. It entails general evidence guidelines for computers, such as shutting down the computer, documenting the hardware configuration of the system, transportation of the computer system to a secure location, making backups of hard drives and floppy disks, authentication of data and originality, and also a comprehensive guide to the legal issues that arise when seizing computers.

According to *Computer Forensics World,* (2010), technological crimes centre mostly on computer crime. These include offences such as theft of marketing information, theft of intellectual property, money laundering, crimes involving drug trafficking, people smuggling, terrorism and pornography. As the number of people with computer skills increases, the battle to keep networks safe grows, including the challenges for the legal systems to be prepared to deal with the many aspects of computer-related crimes and those who are involved in committing such crimes.

According to O'Brien and Marakas (2009:625), computer crime is the actions of criminals accomplished through the use of computer systems, especially with internet to defraud, destroy, or make unauthorized use of computer system resources. *Computer Crime,* (2010) demonstrates that as cyber-crime has become widespread, and a threat to individuals, businesses, financial institutions, governments and nations, cyber forensics seeks to obtain electronic crime evidence that will stand up in a court of law. Therefore, cyber-crime investigators should be prepared to seize computer evidence without compromising it.

To address the problem of seizing computers without compromising evidence, the following aspects are discussed: computer crime, computer forensics, computer evidence and its nature, the

computer crime scene, handling seized equipment, collecting computer evidence, preserving and maintaining a chain of custody, and legal aspects impacting on law enforcement of cyber-crimes.

3.2 COMPUTER CRIME

O'Brien and Marakas (2009:522) demonstrate that computer crime poses serious threats to the integrity, safety and survival of most business systems. Therefore, the development of effective security methods becomes top priority. The authors further draw attention to the definition of computer crime by the Association of Information Technology Professionals, as including the following: "the unauthorised use, access, modification, and destruction of hardware, software, data, or network resources, the unauthorized release of information, the unauthorised copying of software, denying an end user access to his or her own hardware, software, data or network resources, and using or conspiring to use computer or network resources to obtain information or tangible property illegally". The researcher fully agrees with the author's detailed definition, which includes all the aspects of computer crime.

Computer Forensics World, (2010) describes computer crime or cyber-crime as any crime that involves a computer and a network, where the computers may or may not have played an instrumental part in the commission of a crime. According to *Computer Crime,* (2010), these are high-profile crimes such as hacking, copyright infringement, child pornography, child grooming, espionage, financial theft and other cross-border crimes.

Bologna (1989:1) draws parallels between common law crimes and computer crimes, and points out that in common law crimes such as murder, mayhem, larceny, burglary, rape and arson, because of a fairly definitive state of facts, one could know a crime was committed. However, in computer crimes such as fraud, larceny, embezzlement, sabotage of equipment, or information theft, there is nothing known about the type of crime committed, by whom it was committed and even how it was committed. For that reason, how the crime was committed, and by whom, is a matter left for forensic experts to analyse the clues and determine how the crime was committed, with some insight of knowing the culprit.

Swanson et al. (2003:613) believe that computer crime is complicated to become aware of: "the trail is often cold, records may be at a minimum, key people to interview might be left for other jobs, and investigators may not identify key evidence or understand what to ask for due to lack of training or experience". *Brenner,* (2009) states that it is rather more difficult to hypothesise how a remote perpetrator could use a computer to commit a crime. According to *Etter,* (2001:25), the abuse of computer technology may threaten national security, public safety and community well-being, and devastate the lives of affected individuals.

The *Journal of American Science*, (2006:2) states that information security experts put forward that computer crime is also motivated by desire for money, as evidence is found in the occurrence of extortion attempts, theft of credit card details and phishing. Because of this, there are more people who are producing malware to make money. Swanson et.al (2003:613) establish that financial institutions, consulting firms and corporations sometimes do not report fraud or prosecute the offender because of bad publicity involved. In addition to this, these institutions do not want depositors, potential clients and share- holders to think they don't have capacity to manage their affairs. However, this include many home users who are typically unaware of the potential threats from computer crime or those that are not technically inclined to ensure their own security (*Journal of American Science*, 2006:2).

Computer Crime, (2010) agrees with Swanson et al. (2003:613) that the amount of computer crime, and the economic loss to victims, is not precise, as these crimes are seemingly not detected by victims and are never reported to authorities. Based on his experience, the researcher agrees with the authors, that computer crime encompasses a broad range of potential illegal activities. *Computer Crime,* (2010) states that there is consensus among both law enforcement personnel and computer scientists who specialise in security, that both the number of computer crime incidents and the sophistication of computer criminals, is increasing rapidly. *wiseGEEK* (2010) comments that computer crime has become widespread, and computer thieves and pirates have been able to take over the inter-webs. The author is also of the view that identity theft has become a major issue throughout the world, with many options on how to protect oneself – the best way, however, being to avoid using your personal data on the Internet unless it is absolutely

necessary.

According to the *Journal of American Science,* (2010:2), news media continue to report about denial of service attacks, defaced websites, and new computer viruses worming their way through computers. However, there are many other cyber-crimes that are not made public, due to private industry's reluctance to publicise its vulnerability, and the government's concern for security. The *Journal of American Science,* (2010:2) agrees with Swanson et al. (2003:613) about the fear of bad publicity in the industries.

The researcher agrees with the authors that computer crime is a problem, as cyber criminals are seeking opportunities to conduct their illegal activities on the Internet, day in and day-out. Therefore, the computer is the tool that a criminal uses to commit a crime, or it can be a victim of the committed crime. Mendell (2004:25) argues that computer crime is not just about technology, but matters most about people, no matter how sophisticated the security measures of the computer equipment are. The author further explains that crime will occur, due to human error and other potential vulnerabilities.

3.3 COMPUTER FORENSICS

According to Sheetz (2007:2), the term 'forensics' is often misunderstood, because the television and news media are using it without regard for what it actually means. The author explains that 'forensics' is a Latin term that means "belonging to, used in or suitable to courts of judicature or to public discussion and debate." Forensics exists on its own, independently of any specific field of study; for example, forensic entomology is the scientific study of insects, with the goal of introduction into court. It is the same with forensic psychologists who examine the mental condition of people, to offer scientific evidence in court. Computer forensics is therefore the scientific study of computers in a manner consistent with the principles of the rules of evidence and the court rules of procedure.

Wiles, Cardwell and Reyes (2007:2) is of the view that computer forensics is "the preservation, identification, extraction, interpretation and documentation of computer evidence". This view is

supported by Vacca (2002:3), who believes that computer forensics deals with evidence from computers, which is enough and trustworthy to stand up in a court of law, and be unarguable. The researcher agrees with the authors, based on his experience and knowledge acquired from literature. Therefore, computer forensics provides forensic investigators with an understanding of reconstructing a crime after an incident has occurred. Ultimately, the goal of computer forensic investigators is to determine the nature of events about a crime, and to find the offender by making use of a structured investigative system. It is very important for forensic investigators to keep in mind, or to apply, the authenticity and reliability of the evidence, for it to survive in a court of law (Wiles et al., 2007:3).

Once again, the researcher maintains that there is no difference between computer forensics and computer crime investigations. The words are, rather, used by different people to mean the same thing. Wiles et al. (2007:6) state that computer crime is any illegal act involving a computer, its system or its applications. Therefore, cyber-crimes are crimes committed by individuals, and an investigator must make use of the rules to track and prosecute cyber criminals.

3.3.1 Computer investigative skills

Casey (2002:7) explains that when a person deals with data held in a computer, as evidence, such a person should be qualified to do the task and to testify, elaborating the importance and the involvement of their actions. Based on his experience, the researcher supports the view, because computer crime investigators may encounter a variety of incidents requiring computer investigative skills, depending on the situation. Vacca (2002:4) believes that the level of experience of the investigators where there is a criminal case involved, has to be proper. He believes that in an event where computers are dealt with by anyone, instead of by a trained and experienced forensic investigator, the value and credibility of that evidence will be tainted.

Davis et al. (2005:58) persuasively argue that seizure of computer evidence is the most important part of the investigation. It does not matter how good the analysis and procedures; if the evidence was not properly collected, it is a waste of time and resources. Casey (2000:7) comments that seizing, preserving and analysing evidence stored on a computer, is a massive challenge to

investigators. Wiles et al. (2007:6) state that forensic investigators should keep to certain stages and rules. Fisher (2004:193) urges that an expert should be consulted to seize a computer. Mendell (2004:242) agrees with Fisher (2004:193) and Vacca (2002:4), that levels of skills to deal with computer evidence should be assured, inasmuch that no computer investigator should arrive at the witness stand without having a clear understanding of investigation.

The four SAPS cyber -crime technician participants were asked in a case where it is necessary to seize a computer, to explain briefly what type of person they think should seize a computer. One of the participants believed that a person should be trained to seize computers. Another participant said computers should be seized by cyber-crime technicians. The other participant said computers should be seized by people trained to seize computers. The fourth participant further explained that it would be better if all stations could have a trained first respondent. A first respondent is the person who is trained to protect a scene of crime. The participant further pointed out that people who were not trained to seize computers, attended most scenes. That was the reason for the other participant to suggest that all police stations should have first respondents.

The fact that SAPS Cyber- crime Technician who are not trained are attending to computer crime scenes, is of great concern, because it can have the effect that valuable evidence can be lost in the process seizing evidence. One of the four SAPS Cyber- crimes technicians had no training at all but had attended the scene, while another had some elementary training acquired privately. This information was confirmed during interviews by these two participants.

3.4 COMPUTER EVIDENCE AND ITS NATURE

Casey (2002:11) explains that computer crime investigators are faced with the challenge of evidence dynamics. The author further explains that mean the influence that resulting in changes, relocating, obscuring, without being done intentionally, between the time of removal evidence and time of making a decision about it. A computer can be a source of evidence even if it is not directly used for criminal purposes. It is an excellent device for record keeping, particularly the power to encrypt the data, and if this evidence can be obtained and decrypted, it can be of great

value to criminal investigators (*Computer Evidence*, 2010). According to wiseGEEK (2010), computer evidence is data that is harvested from a computer's hard drive and is utilised in the process of a crime investigation.

wiseGEEK (2010) persuasively argues that computer evidence is relatively easy to be corrupted or destroyed. For that reason, forensic experts go to great lengths to secure and protect computers that are seized in the investigation process. According to *NTI*, (2010), computer evidence is quite unique, compared with other forms of documentary evidence, and is very fragile. wiseGEEK (2010) further explains that computer evidence requires great care, and must be dealt with under highly controlled circumstances by professionals who are specifically trained in the process. Bologna (1989:1) agrees with *NTI,* (2010), that computer evidence is the matter that is left in the hands of experts who have specialised knowledge. *Search Security,* (2010) also agrees with *NTI,* (2010) and wiseGEEK (2010), that computer evidence is a unique and exclusive technique when compared with other forms of traditional documentary evidence, and is extremely fragile. *Computer Forensics,* (2010) states that data on computers is volatile, as it changes easily or can be destroyed by simply clicking the mouse in the wrong place.

ACDL Digital Library, (2010) describes data that is stored on, or transmitted by computers, as digital evidence. A complete definition of digital evidence is provided in Chapter 1, paragraph. 1.5.4 of this dissertation. *Herschensohn,* (2005) also defines digital evidence as any data stored or transmitted using a computer that supports or transmits using a computer that supports or refutes a theory of how an offence occurred, or address critical elements of the offence.

Casey (2004:22) believes that digital evidence exists in abundance on open computer systems, communication systems, and embedded computer systems. In addition to this, Wikipedia the free encyclopedia (2010) explains that computing is primarily based on the binary numerical system, and computers interpret binary digital data as information. *Computer Forensics,* (2010) comments that computer evidence has both a physical component (storage media) and a non-physical component (electromagnetic impulses and magnetic orientation).

Casey (2003:15) believes that computer evidence as a form of physical evidence creates many challenges for forensic investigators, because it is a messy, 'greasy' form of evidence that can be very complex to handle. However, the author points out several features that computer evidence has, to lessen this problem:

- Computer evidence can be duplicated exactly, and a copy can be examined as if it were the original.
- With the right tools it is very easy to determine if computer evidence has been modified or tampered with, by comparing it with an original copy.
- Computer evidence is difficult to destroy. Even when a file is deleted or a hard drive is formatted, computer evidence can be recovered.
- When criminals attempt to destroy computer evidence, copies and associated remnants can remain in places that they are not aware of.

The researcher agrees with the author on the features of computer evidence. The challenge for investigators is to be familiar with all these features when dealing with computer crime. Sheetz (2007:26) points out that when dealing with evidence, the underlying principle is admissibility of the evidence to ensure that it is accepted by the court. The reliability of the evidence is also an important requirement. This author is of the view that securing computer evidence is not an easy task, because computers can do a large number of things behind the scenes. It is important that investigators understand computer evidence, to ensure that cases are prosecuted with reliable evidence.

3.5 TYPES OF DATA STORAGE MEDIA

According to *Computer Forensics World*, (2010) there are many types of storage media such as floppy disks, hard disks, zip disks, jazz disks, Bernoulli cartridges, magnetic tape, magneto-optical cartridges, CD-ROM, CD-R, CD-RW and DVD networks. The *FBI Law Enforcement Bulletin*, (2004) is supported by *Computer Forensics World*, (2010), in that there are many types of computer data storage media, of which some are physical and some non-physical. Data *Storage Device*, (2010) points out that computer data storage, also called memory, refers to computer components and recording media that retain digital data used for computing, for some

interval of time. The *Data Storage Media*, (2010) comments that these storages are divided according to their distance from the central processing unit – for example, primary storage (logic unit, registers, cache memory, memory bus, main memory) and secondary storage (mass storage, removable media drive, removable medium).

Burd (1996:23) believes that the storage volume of a computer system must be large, for a number of reasons. These include, among others, the need to store intermediate processing results; programs that are currently executed – and those that are not; data used by currently executed programs; and, data that will be used by programs in the future. However, Wiles et al. (2007:278) demonstrate that a crime scene with a huge storage capacity will surely impact negatively on the ability of the investigator.

The four SAPS cyber-crime technician participants were asked what impact a computer crime scene with a huge storage capacity would have on the ability of the investigator. Two participants believed that it would be a very complex situation to deal with, as it might require more resources. Another participant indicated that he had no clue, due to his inexperience in such cases. One participant made it clear that it was always a problem, and explained further that, for example, if they needed to seize computers in a block of flats, they would need manpower and more trained personnel to seize the computers and peripherals, and then also have enough storage space to store the seized computers. The participant explained further that they were unable to buy trillions of terabyte hard drives to store evidence and make copies.

The researcher agreed with the participants, and is of the opinion that all these problems mentioned by the participants may jeopardize an investigation, and have a negative impact on the solving rate of computer crime. Computer evidence is fragile, meaning that it could be destroyed easily if not handled correctly.

3.6 TYPES OF COMPUTER EVIDENCE

Vacca (2002:123) explains the importance of knowing the different types of evidence, and

failure to know them might be very costly. He further explains the five characteristics for the evidence to be useful and admissible: authentic, complete, reliable and believable. Casey (2000:47) believes the view that investigators have to be aware of the various types of computer evidence. He states that investigators must be able to recognize the hardware containing computer evidence, and be able to establish what information can help to reconstruct a committed crime. The *FBI Law Enforcement Bulletin*, (2004) states that computer evidence can take the form of data digitally stored as text files, graphics files, sounds, motion pictures, databases, temporary files, erased files, and so on. *Computer Forensics*, (2010) also points out that computer evidence can be financial records, word-processing documents, diaries, spreadsheets, databases, e-mail, pictures, movies, found files, and so on. *Hershensohn* (2005) agrees with *Computer Forensics World*, (2010) and the *FBI Law Enforcement Bulletin*, (2004), that computer evidence found as e-mails, electronic documents, spreadsheets, databases and other forms of digital evidence, form the essence of the evidence in a given dispute and/or crime. *NTI*, (2010) supports the view that computer evidence forms the crux of the evidence in a given dispute, and is relied upon more and more in criminal and civil litigation actions.

3.7 COMPUTER CRIME SCENE

Casey (2000:2) states that computer crime scenes present the technical details that are essential in understanding the exact aspects of computer evidence. Fisher (2004:193) points out that when one comes across a computer or any type of computer equipment or data devices at a crime scene, it is essential to keep in mind not to be in a hurry. Steel (2006:12) believes that the computer investigator's crime scene is probably wider than that of the traditional investigator. This view is supported by Bologna (1989:1) when he makes a comparison of the two scenes of crime in that the computer crime scene is a factor left to forensic experts. Fisher (2004:193) explains that an expert should be consulted to analyse and locate pertinent data, for the case to be proper and legal. *Viridis*, (2010) agrees with Bologna (1989:1), that a computer crime scene has different standards compared with that of a traditional crime scene. *Crime Scene Investigator Network*, (2010) states that the goals and objectives of investigating a computer crime scene are the collection, preservation, packaging, transportation and documentation of physical evidence left at the scene.

The four SAPS cyber-crime technician participants were asked whether they were in possession of a set of rules or guidelines to deal with a computer crime scene, and if the answer was 'yes', they had to explain the guidelines. All the participants said 'yes', there were guidelines, and explained as follows: Three participants stated that there are guidelines which can be found on the Internet and in books on computer crime. One participant believed that there are guidelines, but it was not clear enough to cover everything. The participant said they do not have a SAPS training manual. In addition to this, the training they receive from the SAPS is very basic, and is based on A+ and N+. The A+ and N+ are certificates offered by computer institutions such as Damelin and CCS IT Training. Moreover, the participant said the training they receive is the effort of individuals at their head office. The participant believed that the knowledge they have is acquired through their own efforts. For example, the participant underwent advanced training, but this was due to the efforts of the participant, and not that of the SAPS cyber-crime unit.
The researcher learnt from the literature study that cyber-crime training is very expensive, and it is difficult for the criminal justice systems, worldwide, to retain qualified employees. The comments of the participant attested to that kind of situation.

Steel (2006:12) demonstrates that to deal with a computer crime scene, the following steps should be carried out properly:

3.7.1 Identifying of a computer crime scene

Steel (2006:12) states that identifying a computer crime scene may not be straight forward. The author explains that it may require detailed research just to understand where to look, because the remote character of computer evidence gives out extra tasks to the investigator. Casey (2004:216) is supported by Steel (2006:13), in that the investigator must be able to recognise the hardware. For example, the scene may be spreading over and be composed of multiple server rooms, offices and communications closets. Therefore, the investigator must be able to determine which evidence locations are real physical scenes that need to be secured, and which logical evidence has to be analysed and secured logically; these might be a router in a remote or locked communications closet.

Viridis, (2000) and *Crime Scene Investigator Network*, (2010) state that there are many products that can hold computer evidence – for example, telephones, hand-held devices, laptops, larger servers, mainframes, routers, firewalls, and other network devices. In addition to this, there are many forms of storage media, which include compact disks, floppy disks, magnetic tapes, high capacity flip, zip and jazz disks, memory sticks, and USB storage devices. Steel (2006:13) persuasively argues that the physical crime scene can be in another organisation, or in a private residence, or in another country which may or may not have similar computer crime laws. Casey (2004:78) states that there are borders which are transverse in the commission of computer crime and the claim of jurisdiction of the laws governed by different states. The authors point out that a specific physical crime scene might not exist. For example, the perpetrator might be using a laptop at home and at work, and the location where an action was taken may determine what relates to the business place.

Johnson (2006:5) believes that it can be a real challenge for investigators to detect digital or electronic evidence, because its evidentiary value may be hidden through the use of steganography and or encryption. Another challenge, according to this author, is the global nature of computer evidence, where criminal enterprises operate from different nations throughout the world, creating problems with jurisdiction. The author refers to an attack on the Citibank in New York, where FBI members had to examine banking systems in seven different countries. The researcher agrees that the computer crime scene is often wider than the traditional crime scene. It is not an easy task to search computer files for evidence, as files can move all over the world in seconds.

The four SAPS cyber-crime technician participants were asked if there was a possibility that storage devices might not be located on the premises where the seizure is conducted. Three of the participants said ‘yes’. One of them said that computer crime is a cross-border crime. The second participant said that a computer could be connected to a server from another town or country. A third participant said that computers are connected to the Internet, which is covering the whole world. The fourth participant did not know.

Based on the literature study, the researcher agreed with the three participants, that storage devices may not be located on the premises where the seizure is conducted.

3.7.1.1 Suggestions to identify computer crime scene

Lee (2001:261) explores that many jurisdictions are considerably behind the learning curve, and need to quickly put money into significant resources for equipment, training and related resources, to combat computer, Internet and other forms of high-tech crime. Casey (2004:216) believes that exposure to different kinds of computing environments is necessary, to develop expertise in dealing with computer evidence. The author states that local computer science departments and Internet service providers may provide a lesson of their facilities. The author further argues that visiting local computer stores, university laboratories and internet cafes, can be very helpful. The author comments that most computer manufacturers and supplies have websites with detailed pictures and functional specifications of their products. Computer investigators therefore make use of such information to gain better understanding of the variety of hardware. The author believes that it is necessary to know the type of hardware that might be dealt with when approaching a crime scene, as different tools and expertise are required for terabytes of storage versus miniature systems.

According to Steel (2006:13), a possible location for a physical crime scene is the true location where the suspect initiated a digital connection. Crime Scene Investigation (2011) states that knowing where the location, type and quantity of the equipment to be seized are, can reduce the amount of frustration and delay experienced during the raid.

According to Steel (2006:15), performing remote research is necessary to gather more information about the location and to reveal the type of systems in question. In addition to this, special adapters or devices needed on-scene will be known by the investigators.

3.7.2 Secure the crime scene

eHow, (2011) maintains that the most important step is that people need to be removed from the area where equipment will be seized. Steel (2006:17) is supported by *Viridis*, (2010), in that unauthorized people must be removed and the area be cordoned off or locked. Steel (2006:17) states that people who are part of the investigation should sign into the logbook before entering and leaving the crime scene, and include items that are leaving the area, before being removed from the scene.

The *National Institute of Justice*, (2010) states that investigators should ensure that the integrity of both digital and traditional evidence is preserved. In addition to this, the institute maintains that offers of help or technical assistance from any unauthorized individual should be refused, to ensure that the condition of the electronic device is not altered. Swanson et al. (2003:614) state that removing unauthorised people is of high priority, to prevent tampering with, or destruction of, computer evidence.

3.7.3 Documenting of the computer crime scene

According to Mandia and Prosise (2003:199), failure to adequately document activities when attending the scene, is the most common mistake on the part of the computer investigators. Steel (2006:18) describes the documentation of the scene as the most important action in the field of computer forensics. He believes that in documenting the scene, two individuals are best: one person processes the scene while the other is responsible for documenting everything found on the scene. *Rude*, (2000) is supported by Steel (2006:18), in that there must be people working together to document everything that goes on, who did what, how, why and what time, at the scene. *eHow*, (2011) supports the view that the scene must be documented and also photographed, including taking photographs of data and electronic devices. *Field Guide*,*Part Six*, (2011) agrees with *eHow*, (2011), that the crime scene has to be documented and its layout be photographed, to accurately map the scene layout and the location of all evidence found. Steel (2006:19) gives the following brief analysis of items to be photographed at a computer crime scene:

- Computer screens: The current screen must be photographed using a still camera with a

high resolution, in order to read text where it is necessary.

- Network connections: The connections to and from the computer must be photographed very closely, to capture the details of the connections that will also prove that the computer was connected to a specific network or phone at the time of arrival. A video camera must not be used to take photographs at the crime scene, as images may not be viewable due to 'a different' sampling rate' of the camera and the refresh rate of the screen.
- Peripheral connections: Connections to peripherals must be photographed at very close range. This will help to reassemble and prove the connection that will be needed later.

3.8 SEIZING COMPUTER EVIDENCE

Sheetz (2007:27) explains that the seizure process begins with the preserving of the evidence to ensure that the evidence is not changed until presented in court. The author points out that preservation of computer evidence can be difficult, because the evidence is not always apparent. For example when a cheque in a fraud case is seized, it can be seen, recognised, touched and manipulated, but when a laptop computer is seized, the evidence is not visible until the laptop is turned on. The problem is that the evidence on the laptop can change when the computer is turned on – the same as when the computer is turned off. It is for this reason that investigators must understand that doing anything to a computer runs the risk of changing evidence. Any changes to evidence must be documented and explained in court.

When there is a computer involved, or suspected to be involved, in the commission 30 crime(s), such a computer has to be seized in acquiring the evidence. Wiles et al. (2007:266) demonstrate that the challenge for forensic investigators is to collect computer evidence from the scene for further examination. They further explain that the pertinent question is whether to seize all the hardware on the scene, or to determine if the exact copy of the evidence can serve the purpose of an investigation. Casey (2000:15) supports the view that seizing computers require a specific approach, depending on the situation. For example, if a computer contains little pieces of evidence, investigators might not be authorized to collect the whole computer. If the computer is key in a crime, a warrant will be obtained to seize the entire computer. The researcher also

believes that the issue regarding the computer as the evidence against the data as the evidence has a major effect on how to seize evidence at the scene and in the laboratory.

The four SAPS cyber-crime technician participants were asked what would be considered as a challenge in seizing computer evidence. One participant mentioned the shortage of manpower to manage the entire system, and that it is also a challenge to understand the type of computer system. Another participant believed that proper procedures were not followed, because they did not seize computers as cyber-crimes investigators all the time, and because, more often, computers were brought to them for examination. One of the participants believed it was a big challenge to start the seizure, and when they started they faltered. One participant said the challenge is that you can lose the evidence by clicking a wrong button.

The researcher agreed that proper procedures must be followed, and computer evidence is highly volatile as emphasized in the literature study. It is evident from the answers of the participants that it is a real challenge to seize computer evidence.

The SAPS cyber-crime technician participants were asked whether they had any suggestions to solve these problems. One of the participants believed that everyone dealing with the seizing of computers needs to be trained for the job. Another participant said that the key is to follow the correct procedures. The third participant said that computer systems are changing daily; therefore, they should work and be trained accordingly. The fourth participant said that training must be given timeously in order to understand more, and also that enough resources need to be organised. The researcher agreed with the participants, as it had been revealed by the literature study that only trained people should seize computers and work on a computer crime scene.

According to the *National Institute of Justice,* (2010), there should be guidelines for seizing computer evidence, which will also not be in conflict with the requirements of the law. For example, evidence which has been identified as contraband, such as child pornography, may require special consideration such as specific contraband-related seizure and search warrants. Swanson et al. (2003:614) state that computer crime evidence will be seized by the execution of

a search warrant – which must include information about the computer, and other peripherals, that may be of concern in the investigation process.

Steel (2006:19) persuasively argues that since computer evidence has two parts, it has to be processed accordingly. He states that these parts are physical and logical evidence. This view is supported by *Field Guide*, *Part Two*, (2011), in that these are two broad areas which are distinguishable. They comment that when the investigator arrives at the computer crime scene, the first task is to recover and process physical evidence. Secondly, it will be to access data sources on unseized stuff such as log files and databases, to gather information that may give some evidence of something.

Steel (2006:19) points out that physical evidence is best left to people who are trained to deal with it. However, he believes that logical evidence at the crime scene becomes the responsibility of the computer investigator to take over in packaging and handling of logical evidence components. Steel (2006:20) agrees with Swanson et al. (2003:614), that there are items of interest which are considered to be part of physical evidence. These include the following:

- Pieces of paper found with computer equipment
- Papers with user names or passwords should also be collected.
- Searching for keys to laptops or locked drives under desks or hidden in plants.
- Information about the computer, storage devices, floppy disks, tape back-ups, modems, programs, software, manuals, hard copy output, and anything suspected to be useful to prove the case at hand.

3.8.1 Legal guidelines relating to seizing computer evidence

The researcher knows from experience and through literature study that there is a set of rules and procedures that govern the actions of investigators with regard to the seizure of computer evidence. It is therefore essential for investigators to have sound knowledge of these rules and procedures. This clear understanding of such rules and procedures will help to avoid the inadmissibility of evidence as a result of unconstitutional infringement of the rights of individuals.

The four SAPS cyber- crime technician participants were asked about the legal guidelines to keep in mind when seizing computer evidence. One of the participants said there must be an application for a search warrant with the details of computers to be seized. The other participant mentioned that a search warrant is needed. The third participant also mentioned a search warrant with the address and particulars of items to be seized. Another participant said one must have a search warrant for the things that would be seized.

The researcher agreed with the participants, that the search warrant is needed to enter a premises or access and obtain information that is needed for an investigation. The participants did not mention any other legislation or legal guidelines.

The following legislation is important to any person who has to deal with computer evidence:
Section 86 of the Electronic Communications and Transactions Act 25 of 2002 (South Africa, 200a) stipulates as follows:

- Section 86(1) describes hacking as unlawful access and interception of data as a criminal offence.
- Section 86(2) applies to unauthorised interference with data, such as monitoring of data.

Also, the Computer Evidence Act 57 of 1983(South Africa, 1983) provides for authentication of computer-generated documents. These are some of the legal rules which investigators must keep in mind in the process of investigation and seizing of computers. Failure to do so would amount to unauthorisation and inadmissibility of evidence in a court of law.

The researcher believes that there should be a strong relationship between the prosecutor and the computer investigator, because there are many technicalities involved. However, the prosecutor, from a legal point of view, can direct the computer investigator in their investigation. Cyber-crime is regarded as a new type of criminal activity, as the Internet has become available for online users worldwide. Therefore, the types of criminal offences committed online, and the laws that must apply to ensure a successful prosecution, should be known by all computer

investigators.

The following is the legislation that is of vital importance to investigators of computer crime:

- Section 82(1) of the Electronic Communications and Transactions Act 25 of 2002(South Africa, 2002) stipulates that cyber investigators, with the authority of a warrant, may enter any premises, or access information that has a bearing on an investigation. These powers include the authority to search premises or information systems, and search a person or premises if there is reasonable cause to believe they are in possession of an article, document or record with bearing on the investigation.
- Section 82 of the Electronic Communications and Transactions Act 25 of 2002(South Africa, 2002) is not in conflict with section 14 of the Constitution Act 108 of 1996(South Africa, 1996) which guarantees the right to privacy as long as the action taken is within the regulations of the law, as it is common knowledge that there are no absolute rights in terms of the Bill of Rights.
- Section 90 of the Electronic Communications and Transactions Act 25 of 2002(South Africa, 2002) gives South African courts the jurisdiction to try offences where such offences are committed in the Republic of South Africa.
- Section 86 of the Electronic Communications and Transactions Act 25 of 2002(South Africa, 2002) provides a description of cyber-crimes as follows:
- Section 86(1) describes hacking as unlawful access, and interception of data as a criminal offence.
- Section 86(2) applies to unauthorised interference with data, such as monitoring of data.
- Section 86(3) and 86(4) deal with anti-cracking and -hacking law. The law stipulates that the selling, or designing or producing of anti-security, circumventing technology, will be a punishable offence.
- Section 86(5) states that e-mail bombing and spamming are criminal offences.
- Section 87 of the Electronic Communications and Transactions Act 25 of 2002(South Africa, 2002) mainly introduces cyber-crimes of extortion, fraud and forgery.

There are other statutes that are applicable in the seizure and prosecution of cyber-crimes, such

as the Computer Evidence Act 57 of 1983(South Africa, 1983). This Act provides for authentication of computer-generated documents. Also, the Regulation and Provision of Communication Related Information Act 70 of 2002(South Africa, 2002) provides for the collection, preservation and reporting of electronic information. In general, one would consider that cyber-crimes are not limited to the activities contained in the Electronic Communications and Transactions Act.

3.8.2 Evidence collection kit

Marcella and Menendez (2008:242) believe that the type of investigation should inform the cyber forensic investigator. However, due to the fact that tools and technology often change, the cyber forensic investigator must be ready, and stay abreast of technology with the best tools to carry the task. Steel (2006:20) persuasively argues that computer crime scenes are not identical. For this reason, the appropriate tools should be made available.

The four SAPS cyber-crimes technician participants were asked if there were a set of tools to seize or collect computer evidence, and if the answer was 'yes', what those tools were. All the participants agreed, and said 'yes'. One participant mentioned a set of screwdrivers, in case of removing a hard drive. Another said it depended on the situation as to what would be needed, while another participant said it is necessary to have a mobile kit suitable for dealing with computers. One of the participants believed that cyber-crime investigators must be ready with the best tools to carry out tasks at any time. From his own experience and from the literature, the researcher has learnt that crime scenes are not identical, and appropriate tools should be made available.

Marcella and Menendez (2008:242) agree with Steel (2006:20) that, at least, the following tools should be included in any forensic response toolkit:

- Latex gloves: These gloves protect a person against irregular edges when handling computers, and from leaving fingerprints all over the place.
- Security tape: This tape will be used to cordon off the crime scene when the need arises.

- Evidence tags and labels: These will be used to mark evidence found at the crime scene.
- Cable ties: These cable ties are used to tie labels to a piece of evidence.
- Bolt cutters: These help to break key locks quickly.
- Shapies: Are used on Compact Disk-recordable, evidence tag or surface.
- Anti-static bags and evidence bags: These are containers used to keep evidence found, such as floppy disks and laptops. Anti-static bags protect computer equipment from static electricity. Evidence bags are temper resistant, and their labels are unfasten able or detachable.
- Digital camera: A digital camera with a time and date stamp will be suitable – also a 35mm lens that is able to zoom in and zoom out to capture close-ups of network connections, components and cables.
- Forensic notebook: A book with irremovable pages, and numbered.
- PC Toolkit: An advanced toolkit will be good to get everything needed.
- Forensic laptop, hard disk and adapters: A laptop with external firewire hard disk and adaptors such as ADP 3, adaptor SCSI3 to SCSI1, ADP32 adaptor SCSI3 to high density, fast block unit blocker, log cube and software.

3.8.3 Sequence steps to seize computers

Sheetz (2007:29) explains that when investigators approach the scene of a case involving digital evidence, they should follow the rule to "change nothing" – similar to the Hippocratic Oath which states "first do no harm." This rule of changing nothing and documenting everything is the tool that should guide the seizure of computer evidence.

Wiles et al. (2007:273) state that seizure of computers used to be done by highly trained specialists. However, the increase of computers and their involvement in criminal efforts made it impractical. The challenge facing law enforcement is to give investigators a high degree of training required to deal with cyber-crimes. The authors outlined the following steps that investigators should be trained in:

- Digital Media Identification.
- Minimizing the crime scene by prioritising the physical media.

- Seizure of storage devices and media.

Swanson et al. (2003:615) believe that great caution should be taken when computers are seized, to ensure the correctness and reliability of the evidence. Through the literature study, the researcher found some common steps to be followed when seizing computers. The researcher also established that listing the steps of each author would result in a massive document. For this reason, the researcher decided to write a statement from each author, and list the common steps thereafter. Fisher (2004:193) gives a brief but analysis of the steps to be remembered in seizing computers. Marcella and Menendez (2008:286) also give a summation of the steps to be followed when seizing computers, and are not in dispute with Fisher (2004:193). The researcher found a number of Internet sources covering the steps to be taken when seizing computers. These sources are: the *National Institute of Justice*, (2010), *Steps to Seize Computers*, (2010), *Crime Scene Investigator Network*, (2010) and *Intratec Data Recovery*, (2010). These sources agree with Fisher (2004:193) and Marcella and Menendez (2008:286) regarding the steps to be followed when seizing computers. Steel (2006:23-24) and *Field Guide*, *Part Two*, (2011) also state similar steps to be taken when seizing computers. Wiles et al. (2007:299) believe that it is not possible to present one correct way of seizing computer evidence, but there are basic steps that tie all seizure processes together. The researcher agrees with the authors that there are many approaches, depending on the complexity of the scene and the skills of the investigators. The following are basic steps which are important in the process of seizing computer evidence, as mentioned by the authors:

3.8.3.1 Step 1: Photographs and locations of the equipment at the crime scene

Steel (2006:23) and Fisher (2004:193) state that before disconnecting cables, all connectors must be labeled and photographed in their positions at the crime scene. The authors believe that labeling the cables and noting them in the logbook, will also help when reassembling the computer system.

3.8.3.2 Step 2: Document computers, devices and media

Fisher (2004:193) is supported by *Field Guide*, *Part Six,* (2011), in that photographs of the

computer screen, the front, back and sides of the computer, and peripherals attached to the computer, must be taken and be documented.

3.8.3.3 Step 3: Determining whether or not to power down computers

Steel (2006:23) agrees with Fisher (2004:193), and is supported by *Field Guide, Part Six*, (2011), in that it is very important to determine if the computer is connected to the network or not, before it can be powered off. If it is connected to the network, it must be dealt with by a trained person. For example, a mainframe or server that supports the operations of the organisation should not be powered off. Instead, a back-up of the RAM must be done before proceeding, and all actions taken be recorded in the logbook.

3.8.3.4 Step 4: Power down running computers

Steel (2006:23) is supported by *Field Guide, Part Six*, (2011), in that a decision to shut down, unplug or to analyse the computer while it is live must be carefully thought. The authors comment that shutting down a Windows system using the shutdown button, will have a negative impact on a forensic investigation. According to Steel (2006:24), the following are the instructions for shutting down the computer system:

- Overwrite sections of the hard disk free space, as information in memory is written to disk.
- Remove the swap file (page file.sys) that stores cached memory, depending on the operating system version and system settings.
- Terminate any running process or applications, some of which may prompt for the saving of data, rendering the information unrecoverable in certain cases.
- Alter date and time stamps on numerous files.
- Delete temporary files.
- Add entries to the event logs.

Steel (2006:24) explores the possibility that other operating systems may be damaged by improper shutdown, but Windows operating systems are better when they are powered down by unplugging. *Field Guide, Part Six,* (2011) points out that if the investigator is not certain whether or not to power down a live computer, a person with better expertise should be located.

Swanson et al. (2003:615) find evidence that powering down the computer can result in the missing of incriminating files. For this reason, investigators must be careful of installed traps in the machine. For example, a trap can be a custom-written software program aimed at deleting an incriminating data when the computer is booted.

The four SAPS cyber technician participants were asked how the removal of power from a running system would impact on the stored evidence. One of the participants said that one must know whether to pull out a plug or to take out batteries, in the case of a laptop. Another participant said that it is important to determine the type of system being dealt with. One participant said that it is necessary to know the way to deal with running systems – otherwise, evidence would be lost. The other participant said one should just be sure of what one is doing.

The researcher believes that the participants do have an idea of the importance of this action, and that evidence can be lost if it is not conducted in the correct manner.

Steel (2006:24) persuasively argues that the following questions can be helpful to evaluate the decision to do a live analysis or not:

- Is an incident actively occurring on the machine?
- Will capturing data about the incident as it is occurring, be potentially useful? If so, key stroke monitoring, network sniffing and other techniques may be appropriate.
- Find out whether the current incident is destroying data, attacking other systems or executes destructive actions that can be stopped by unplugging.
- Will unplugging alert the suspect?
- Are there current open applications whose contents will be useful in the case?
- Is the information stored in memory likely to be a key part in the investigated case?
- Is that information likely to be more important than the information on the hard disk?

Steel (2006:24) comments that there are additional alternatives between pulling the plug, and doing a live analysis:

- Document the open applications before pulling the plug.

- Evaluate the system remotely.
- Perform a remote forensic duplication (using encase enterprise), and then perform a live analysis.
- Do the critical pieces of a live analysis and then pull the plug.

3.8.3.5 Step 5: Mark and tag all hardware, cables and media.

Fisher (2004:193) is supported by *Field Guide, Part Six*, (2011), in that an evidence tag should be attached to the seized equipment. That helps to identify computers and devices, also the model of the computer, brand name, type, and serial numbers should be properly labeled.

3.8.3.6 Step 6: Prepare computers, devices and media for transport

Field Guide, *Part Six*, (2011) agrees with Fisher (2004:193), that computer evidence should be packaged in cardboard boxes and be labeled with their contents. In addition to this, the use of packing foam and anti-static plastic covers is highly recommended, whenever possible. This includes placing storage media in appropriate containers. *Field Guide*, *Part Six*, (2011) urges that a specific logbook to record the transportation of the seized evidence from the crime scene and at the storage place, be kept. The information comprises the recording of the date and time of departure from the scene, the names of the contents enclosed in the boxes, and the person(s) loading the boxes. On arrival at the place where the evidence will be kept, all evidence should be checked with the person(s) responsible for the storage or laboratory administrator.

3.9 CHAIN OF CUSTODY

Vacca (2002:154) defines the chain of custody as "a roadmap that shows how evidence was collected, analysed and preserved, in order to be presented as evidence in court ". The author further explains that it is quite evident that there is a need to keep a clean record of the chain of custody, and points out that electronic evidence should be trustworthy. The following aspects must be taken into consideration:

- Information has to remain unchanged.
- A complete copy has to be made.
- The copying process used has to be reliable.

- Securing of all media should be assured.

Wiles et al. (2007:8) agree with Vacca (2002:154), in that a chain of custody is an exact documentation of the steps taken with the evidence until it reaches a court of law. The authors believe that the documentation aids in avoiding accusations of tampering, establishes that storage was effected at a legally recognised location, and shows who was in control of the evidence all the time.

The four SAPS cyber-crime technician participants were asked why it is important to maintain a chain of custody of computer evidence. One of the participants said that it is important for the admissibility of evidence in court. Another said that it is to prove the originality of evidence in court. A third participant said it is to prove that the evidence was not tampered with. The fourth participant said it is necessary to prove that the evidence remains the same as it was when it was seized.

Based on his work experience and the literature study, the researcher agrees with the participants that the chain of custody should be truthful about the handling of evidence, in order to be admissible in a court of law. According to Steel (2006:25), the chain of custody mainly deals with maintaining a documented record of the person(s) in control of evidence every time, from collection, during court proceedings and the place of storage. Marcella and Menendez (2008:288) believe that when dealing with the computer chain of custody, general forensic and procedural principles should be applied. These are principles such as preventing actions that can alter evidence, recording actions taken, and that people dealing with computer evidence must be trained for the purpose.

The *Field Guide*, *Part Six*, (2011) suggests the following practical steps in the documentation of computer evidence, to ensure chain of custody:

- An evidence log file must be opened to mathematically authenticate the data on all crime scene computer hard drives and media.
- A bit stream back-up of all crime scene computer hard drives and media must be created

prior to any forensic examination.

Steel (2006:25) believes that the storage of evidence should be access controlled with no more than two persons. The author also comments that this fact must be indicated. Swanson et al. (2003:614) point out that the storeroom must be free from dust, heat and magnetic fields. Fisher (2004:193) supports the view that computer evidence must be kept away from magnetic fields.
The four SAPS cyber-crime technician participants were asked, taking storage after seizure into consideration, under what conditions the computer equipment should be stored.

One of the participants said that computer equipment must be stored in a cool, dry place. Another participant mentioned that there must be adequate ventilation, and the place should be free of dust and electromagnetic fields. The third participant said that the storage must not be humid or hot, because such conditions would have bad results, due to chemical reactions from the components used to design some of the equipment. The fourth participant said that the storage should be spacious, have sufficient light and enough ventilation, and be clean.
The researcher believes that the participants understood the conditions under which computer equipment should be stored.

Steel (2006:25) states that the chain of custody and the supporting documents must be able to prove validity in a court of law. For this reason, the documents must satisfactorily show:

- That the evidence collected is the same as was presented in court.
- That the position of the evidence was known at every point in time.
- That an evidence keeper was apportioned at every point in time.
- That no one except those listed on the chain of custody form, had access to the evidence.
- That the evidence was not mistakenly or intentionally altered as part of the investigation process.

The researcher believes that failure to comply with proper procedures means that valuable evidence cannot be used, and time, effort and all resources will be wasted.

3.10 LEGAL ASPECTS IMPACTING ON LAW ENFORCEMENT OF CYBER-CRIMES

3.10.1 Information from interviews with state prosecutors

The three prosecutors were asked what the legal challenges are that investigators have to deal with when seizing computers. One of the prosecutors said “interpretation of the law”. Another prosecutor believed that a challenge is the interpretation of the Criminal Procedure Act regarding search and seizure. The third prosecutor believed that the challenge lay with technicalities in the interpretation of the law.

The researcher believes that it is imperative that cyber-crime investigators be familiar with all the laws relating to search and seizure of computers, as well as the procedures. The literature study mentioned legal guidelines that govern the actions of investigators with regard to the seizure of computer evidence. For example, section 82(1) of the Electronic Communications and Transactions Act 25 of 2002(South Africa, 2002) stipulates that cyber investigators, with the authority of a warrant, may enter any premises or access information that has bearing on an investigation.

The three prosecutors were asked if there are any challenges facing South African legislation, in terms of regulating cyber-crimes. One of the state prosecutors said ‘no’, and explained that the legislation of South Africa covers all legal aspects regarding cyber-crimes. Another state prosecutor said ‘no’, and stated that South Africa has strong legislation to prosecute cyber offenders – for example: the Electronic Communications and Transactions Act 25 of 2002(South Africa, 2002); Regulation and Provision of Communication-related Information Act 70 of 2002; 4/1/9 Money scams; and, the Criminal Procedure Act 51 of 1977(South Africa, 1977). The third state prosecutor said ‘no’, and drew attention to the abundance of red tape which forms stumbling blocks in the path of the investigation. According to this state prosecutor, these ‘red tapes’ are as follows:

- Following up of Internet protocol addresses speedily.
- The application of section 205 of the Criminal Procedure Act 51 of 1977(South Africa, 1977) which allows investigators to have access to information about suspects in the investigation

process takes too long.

It is clear to the researcher that there is room for improvement in the procedures that are to be followed. The three state prosecutors were asked what, in their opinion, could be done to improve the success rate of cyber-crime prosecutions. One of the state prosecutors believed that section 205 of the Criminal Procedure Act 51 of 1977(South Africa, 1977) which allows investigators to have access to the required information, should be substituted by a quicker process. The state prosecutor explained that it would allow cyber-crime investigators to 'track' down the relevant computer used by the offender, speedily, because the process allows offenders to move around quickly, and when the investigators reach the scene, it is already too late. The other state prosecutor said there should be a process of getting information immediately. For example, the prosecutor believed that the FBI (Federal Bureau of Investigations) in the USA (United States of America) is obtaining information with a click of a button, compared with SAPS cyber-crime investigators. Another state prosecutor stressed the need for the SAPS to recruit more cyber-crime investigators for the analysis and seizing of computers. The state prosecutor believed that it takes too long to get results while the suspect is awaiting trial.

The researcher believes that the state prosecutors shared valuable information on the problems with the procedures that investigators have to follow, being too slow, as well as the shortage of cyber-crime investigators.

The three state prosecutors were asked if they considered cyber-crime investigators as successful.

One of the prosecutors said 'yes'. The prosecutor believed that there were positives or successes. However there were challenges, leading to a lack of success – for example, the failure to record seized equipment, such as cellular phones, according to the persons from whom they were seized. Another prosecutor said there was definite success. The third prosecutor said 'yes', but there were challenges too.

The researcher is of the opinion that the problems that were identified with regard to computer

evidence, could be prevented if investigators were properly trained to understand the correct procedures to follow.

The three state prosecutors were asked about their role when dealing with cyber-crime investigators. One of the prosecutors said the role is to guide the investigator to follow the right procedures described in the legislation. Another state prosecutor said the role of a prosecutor is to help the investigator to identify relevant witness statements and documentary evidence which needs to be obtained, and to follow proper procedures. The third state prosecutor said their role as state prosecutors is to give guidance in what the law requires investigators to do.

It is evident that the prosecutors know what is expected of them when dealing with investigators in cyber-crime cases. The support, guidance and assistance of the state prosecutors are of vital importance for the successful prosecution of cases.

The state prosecutors were asked whether cyber-crimes are different from the other types of crimes, and if the answer was 'yes', they had to explain the difference. All of them said 'yes', they are different from other crimes, and they explained as follows: One participant stated that cyber-crime offenders were faceless, and could be unleashed through proper investigation. Another state prosecutor said that cyber-crimes were cross-border crimes. The state prosecutor explained that cyber-crimes required sophisticated knowledge and skills to deal with them. The state prosecutor explained further that cyber-crime could be committed by an offender sitting in another town, country or continent.

The researcher believes that the prosecutors are familiar with the challenges with regard to the investigation of cyber-crime, and that specific skills and knowledge are needed to ensure success.

The state prosecutors were asked if there is any important legislation that in their opinion, cyber-crime investigators should be familiar with. One of the state prosecutors said that all legislation is equally important. Another state prosecutor believed that it is vital to keep in mind all

legislation required for the process of investigation. Another prosecutor said the legislation is what guides investigators in what they should or should not do. For that reason, all legislation is absolutely necessary. The researcher believes that the opinions of the state prosecutors give credence to the literature study.

3.10.2 Legal considerations

The manner in which evidence is obtained by the police is crucial to the legal credibility of the evidence in court. Section 35(5) of the Bill of Rights of the Constitution forms the basis for questioning the way in which evidence is obtained. Section 35(3) of the Constitution provides that evidence obtained in a manner that violates any right in the Bill of Rights must be excluded, if the admission of that evidence would render the trial unfair or would otherwise be detrimental to the administration of justice. However, section 36(1) contains a provision which has become known as the "limitation clause". This section provides that the rights granted by Chapter 3 of the Constitution may be limited by statute or common law if such limitation is reasonable and justifiable in an open democratic society based on freedom and equality.

Sections 20-29 of the Criminal Procedure Act 51 of 1977(South Africa, 1977) prescribe the mechanisms of search and seizure, including search warrant authorisation. Among others are the Police Act 68 of 1975(South Africa, 1975), the Prevention of Organised Crime Act 121 of 1998(South Africa, 1998) and legislation relating to special investigation units. For the purposes of this research it would be very difficult to detail and argue each section, as that would result in a massive document. Nevertheless, these rules must come into play whenever there is seizing of computers carried out by investigators.

In addition to this, section 20 of the Regulation of Interception of Communications and Provision of Communication related Act 70 of 2002(South Africa, 2002) provides for search warrants. The Act stipulates that anyone who needs data messages stored on a computer as part of a criminal investigation will have to apply for a search warrant either in terms of Chapter 2 of the Criminal Procedure Act or the other legislation that provides for search warrants. Furthermore, section 20(b) of the Regulation of Interception of Communications and Provision of Communication

related Act 70 of 2002(South Africa, 2002) allows the state to seize anything referred to as an article that may afford evidence of the commission or suspected commission of an offence, whether within the Republic of South Africa or elsewhere, and also anything that has been held to extend to documents and money and will extend to a computer or hard drive in which data messages are stored.

The warrant must be issued by a magistrate, justice of the peace, judge or judicial officer, and must, as the name implies, be in writing thus, according to Act 70 of 2002(South Africa, 2002). The Act continues to state that the terms in which a warrant is issued may refer to merely copying the data messages or removing a computer or hard drive.

According to Vacca (2002:57), legal issues encompass the problem of having evidence to be accepted in a court of law in order to redress cyber-crime. He demonstrates that the evidence collected should be shown to be untampered with, and every step taken be accounted for. Mandia and Prosise (2003:57) emphasise that appropriate, acceptable use of policies is key in the investigation process. Wiles et al. (2007:271) agree with Mandia and Prosise (2003:57), that seizure should be authorised with a warrant, to comply with the legal requirements. This implies that to seize computers, authorisation, acquisition of computer evidence, and authenticity or originality, are key properties for evidence to be admissible in court.

3.10.3 Authorisation

Seizing of computers must comply with the requirements of the law so that the evidence collected can be admissible in court. *Hershensohn*, (2005) outlines four steps for computer evidence to be legally collected:

- By receiving the permission of the owner, such as written permission of the owner, or by mutual consent as detailed in a contract.
- By means of an order of court in cases involving copyright and other intellectual property disputes.
- By means of a search warrant issued by a court.
- By means of an interception directive issued. Swanson et al. (2003:614) support the view

> that computers ought to be seized by execution of a search warrant. The authors believe that the warrant should contain information about the computer, data storage devices such as internal and external hard drives, floppy disks, tape back-ups, modems, programs, software manuals, user notes, hard-copy output, and any peripherals that may be of concern to investigators.

Wiles et al. (2007:578) emphasise that the search warrant should include the proper authorization to perform on-site examinations of computer equipment such as wireless access devices. The authors believe that detection of wireless access points from a wired network has many advantages. For example, making use of Network Mapper can set automated scripts that search a network on a continuous basis, and that will save time and money.

Casey (2000:216) points out that in order to obtain a warrant, investigators must show the probable cause, and detail the place to be searched, including the things to be seized. He further explains that the judge or magistrate must be convinced that a crime has been committed, that evidence of crime exists, and that the evidence is likely to exist at the place to be searched. This implies that computer investigators have to conform to rules and regulations, when seizing computers, for the evidence to be acceptable in court. Casey (2000:216) persuasively argues that there is no way of imagining a case in which a computer can be seized without a search warrant, because a warrantless search can only be done when there is exigency – which will mean a life-threatening situation.

3.10.4 Acquisition of the evidence

According to *Kenneally*, (2009), the traditional computer evidence environment, evidence searches and seizures, are parallel or similar to that of traditional physical evidence. The author states that practitioners enter the location to be searched, seize computer hardware, and take the hardware offsite where it is digitally searched for potential evidence of crime. However the live-remote methodology does not necessitate taking systems offline or maintaining physical proximity with the target media. Nevertheless, general principles should apply upon seizing computers. *Hershensohn*, (2005) believes that the evidence should not be changed by actions

taken, the person should be trained for the purpose, and actions steps relating to seizure should be documented.

3.10.5 Authentication

Kenneally, (2009) argues that failure to embrace and validate the principles will tarnish the authenticity and admissibility of the resulting evidence. *Hershensohn*, (2005) agrees with *Kenneally*, (2009), that authentication means satisfying the court that the contents of the evidence remained unchanged, and originate from the purported source.

Section 15 of the Electronic Communications and Transactions Act 25 of 2002(South Africa, 2002) stipulates the admissibility and evidential weight of data messages, with regard to authenticity. The Act states that data messages shall be admissible, giving due regard to reliability of the manner of storage, generation and communication, reliability of admission, the manner of maintenance of the message, the manner in which the originator is identified, and any other relevant factor. The Act creates a rebuttable presumption of the data messages and/or printouts which are admissible in evidence.

Section 15(3) of the Electronic Communications Transactions Act 25 of 2002(South Africa, 2002) clearly stipulates the factors that must be considered to determine the importance of data messages, as follows:

- The reliability of the manner in which the data massage was generated, stored or communicated.
- The reliability of the manner in which the integrity of the data massage was maintained.
- The manner in which its originator was identified.
- Any other relevant factor.

The Act also concludes by highlighting that the existence of electronic data regarding authenticity has no exact approach that suits all instances. The reason is that electronic data is in various formats and applications.

According to Wiles et al. (2007:12), the issues relating to authenticity, reliability, and completeness and convincing, are key legal issues that cannot be separated from the practical aspects of computer investigation. The researcher agrees with the authors, that it is very important for investigators to adhere to rules and regulations. There are many rights of citizens which can be infringed in the process of seizing computers. However, certain rights will always be infringed when Acts such as Criminal Procedure Act 51 of 1977(South Africa, 1977), the Constitution, Act 108 of 1996(South Africa, 1996) and Act 70 of 2002(South Africa, 2002) are applied. Therefore, it is very important to provide a transparent view of the seizure and the entire investigative process.

3.11 SUMMARY

The focus of this chapter was on the methods and techniques of seizing computers, without compromising evidence. However, it appears that the seizing of computers is a process with interrelated steps. Concepts such as computer crime, computer forensics, and computer evidence and its nature, were discussed at length.

Steps to approach a computer crime scene also revealed that it is a process requiring specialised knowledge and skills. Handling seized equipment, seizing computer evidence, and preserving and maintaining the chain of custody, also require specialised knowledge. Adequate training has been highlighted in this chapter, to ensure that no possible evidence is damaged, destroyed or compromised by the procedures used. Legal guidelines and procedures must also be taken into consideration to avoid the inadmissibility of the evidence in court. Various sections in a number of Acts guarantee the rights of the citizens of South Africa. There are, however, various pieces of legislation which allow these rights to be infringed, in the best interests of the country. The next chapter contains the findings and recommendations of this study.

CHAPTER 4

FINDINGS AND RECOMMENDATIONS

4.1 INTRODUCTION

The research was conducted because of the problems that the SAPS Cyber-crime Unit is experiencing in the search and seizure of computer evidence. The aim of the research was to determine the role of a computer in facilitating the commissioning of crimes in forensic investigation process, and how computers can be seized without compromising evidence.

The research has shown that the cyber-crime phenomenon has grown tremendously in recent years, and that the computer can play a role in the commissioning of almost every crime. However, various articles pointed out that many stakeholders had less confidence in working with the SAPS in solving cyber-crimes. Problems regarding the capacity of the police, as well as a lack of knowledge and skills, were mentioned.

The findings and recommendations are aimed at improving the procedures that are followed, with regard to seizure of computer evidence. The researcher made use of research questions to spell out exactly what is to be investigated. It assisted the researcher to address the problems that were identified with regard to computer evidence.

The following findings and recommendations are based on information obtained from a thorough literature study and interviews with cyber-crime technicians and state prosecutors.

4.2 FINDINGS

The following are the findings of the research:

4.2.1 Research Question One: What is the role of a computer to facilitate the commissioning of crimes in forensic investigation?

- The research has shown that a computer can play a very important role in the forensic investigation process, when computer technology is used by criminals to engage in criminal

activities.

- The increase of computer technology and the development of the Internet have created opportunities for criminals to commit crimes where computers are involved.
- It became evident that computer forensics is about collecting evidence from computers, and it should be sufficient to make its way into court and be persuasive. It entails the preservation, identification, extraction, interpolitation, analysis and documentation of computer evidence.
- It was revealed that computers and networks could be targets of crime, or used as tools in the commission of crime, and could be incidental to a crime where the offender only uses the computer to advance a criminal end.
- The research has shown that it is of vital importance that investigators be acquainted with the different categories of computer crime, such as the computer as a target, as an instrumentality of the crime, as incidental to the crime, and crimes associated with the prevalence of computers.
- It was discovered that a computer forensic investigation consists of the following basic phases:
- Acquisition – where information and evidence is gathered.
- Authentication – ensuring that the acquired evidence is the same as the data that was originally seized.
- Analysis – that entails the examination and evaluation of the information.
- The research has indicated that the types of data that are of concern in computer forensic investigation are active data that can be seen by the naked eye, archival data which has been backed up and stored, and latent data or information that requires special tools to deal with – it may be information that has been deleted or partially overwritten.
- The scope of computer crime can be summarised as follows: physical crimes such as theft, burglary and terrorism, sexual exploitation, malicious e-mail and cyberspace fraud, alteration of programming codes, malicious code viruses, penetration of operating systems, manipulating input and output flaws, industrial spying, wiretapping and retail computer security.
- It became evident that in cyber-crime cases, much of the evidence is digital – which means

that it is not tangible evidence. The evidence is made up of electronic or magnetic pulses and stored in the form of electromagnetic charges on a disk or tape. It is very fragile and can be compared to a footprint in snow that must be captured before it melts away.

4.2.2 Research Question Two: How can computers be seized without compromising evidence?

- The research has shown that cyber-crime has become widespread and a threat to individuals, businesses, financial institutions, governments and nations.
- It was revealed that cyber or computer forensics deals with electronic evidence from computers which are sufficiently and trustworthy to be accepted as evidence in court; therefore, only qualified investigators can deal with computer evidence.
- It became evident that, in cases of common law crimes such as murder, burglary, rape or arson, because of a fairly definite state of facts, one could know a crime was committed; however, in computer-related crimes such as fraud, larceny, embezzlement, sabotage of equipment or information theft, there is nothing known about the type of crime committed, by whom it was committed and even how it was committed. Forensic experts have to analyse clues to determine how the crime was committed, with some insight of knowing the culprit.
- The research has illustrated that seizure of computer evidence is the most important part of the investigation. It does not matter how good the analysis and procedures: if the evidence is not properly collected, it is a waste of time and resources.
- It was revealed that computer evidence is unique. Compared with other forms of documentary evidence, it is very fragile and requires great care, and must be dealt with under highly controlled circumstances by professionals who are specifically trained in the process.
- It is obvious from the research that computer evidence as a form of physical evidence creates many challenges because it is a messy, greasy form of evidence, and it is therefore important that investigators are familiar with the following features of computer evidence:
- Computer evidence can be duplicated exactly, and a copy can be examined as if it were the original.
- With the right tools it is easy to determine if computer evidence has been modified or

tampered with, by comparing it with the original copy.

- Computer evidence is difficult to destroy; even when a file is deleted or a hard drive is formatted, computer evidence can be recovered.
- When criminals attempt to destroy computer evidence, copies and associated remnants can remain in places that they were not aware of.
- It is of vital importance that investigators are aware of the different types of computer evidence, to recognise the hardware containing the evidence, and to establish what information can assist in reconstructing a committed crime.
- Computer evidence can take the form of data digitally stored as text files, graphics, files, sounds, motion pictures databases, temporary files, erased files, and so on.
- It was established that a computer crime scene presents the technical details that are essential in understanding the exact aspects of computer evidence. The scene has different standards, compared with those of a traditional crime scene, and experts are needed to analyse and locate pertinent data, for the case to be proper and legal
- During the interviews with the cyber-crime technicians, they revealed that they do not have guidelines or a manual on computer crime investigation, in the SAPS, and therefore had to obtain their own guidelines from the Internet and other sources. It is evident that there is a real need for guidelines on computer investigation.
- It was discovered that the SAPS training in cyber-crime is very basic and in adequate; the cyber-crime technicians also indicated a need for advanced training in computer crime investigation.
- It became apparent from the interviews with the SAPS cyber-crime technicians that the SAPS is in need of more cyber-crime investigators, because they experience a shortage of manpower.
- The research has revealed that there are only a few prosecutors trained to prosecute cyber-crime – this is also a challenge.
- The research has shown that a computer crime scene is very complicated: it may require research to just understand where to look for evidence; the evidence may be spread over, and be composed of, multiple server rooms, offices and communication closets.
- It was revealed that the global nature of computer evidence where criminal enterprises

operate from different nations throughout the world can create problems with jurisdiction.

- It became evident that when dealing with a computer crime scene it is very important to secure the scene and remove unauthorised people to prevent tampering with, or destruction of, the evidence.
- It is apparent from the research that failure to adequately document and photograph activities when attending to the scene is the most common mistake that is made by computer crime investigators.
- It is evident that only highly trained specialists are needed to seize computer evidence, because there are various steps and many different approaches that can be followed, depending on the complexity of the scene.
- It was revealed that great care is needed when computers are seized, to ensure the correctness and reliability of the evidence obtained. The cyber-crime technicians indicated that they are aware of this, and to prove it, one of them stated that "you can lose evidence by clicking a wrong button".
- The research has shown that it is essential for all cyber-crime investigators to have a sound knowledge of all the legal requirements relating to seizure of computer evidence.
- During the interviews with the prosecutors who are responsible for the prosecution of cyber-crime, the following important aspects were revealed:
- Cyber-crime is different from other types of crime: the offender is faceless, and the crime can be committed by an offender sitting in another town, country or continent; this makes it complicated to deal with.
- The interpretation of the law with regard to search and seizure, poses a challenge to investigators.
- It is imperative that cyber-crime investigators be familiar with all the laws relating to search and seizure of computers – including procedures thereof.
- "Red tape" forms stumbling blocks in the path of the investigation where Internet protocol addresses needs to be followed up speedily.
- The application of section 205 of the Criminal Procedure Act 51 of 1977 which allows investigators to have access to information about suspects in the investigation process, takes too long, and should be substituted by a quicker process.

- The process that investigators have to follow to obtain information is too slow, in comparison with the FBI, in the USA, that can obtain information with a click of a button.
- There is a need for the SAPS to recruit more cyber-crime investigators, for analysis and seizure of computer evidence.
- Other problems experienced with the investigation of cyber-crime, were the failure to record seized equipment and to maintain the chain of custody with regard to seized computer evidence.
- The prosecutor's role is to assist and guide the investigators to follow the proper procedures as described in the legislation.

4.3 RECOMMENDATIONS

The following recommendations are made:

- The SAPS should recognise the fact that the information society is structured in a manner that depends on computers and networks, and that computer evidence can play a vital role in any type of investigation.
- All police investigators, and other police members, should at least be trained in the basics of a cyber-crime investigation, because the time will come when they will all have to deal with an aspect of cyber-crime in the daily execution of their duties and, specifically, in investigations.
- The SAPS should recruit more cyber-crime investigators to attend to cyber-crime investigations.
- The SAPS should improve their training in cyber-crime as such, to meet the demands of cyber-crime investigations.
- The cyber-crime investigators should receive guidelines on the legal requirements and investigation procedures to enable them to deal effectively with cyber-crime.
- Training manuals and procedures should be updated on a regular basis to ensure that they remain relevant.
- The SAPS and the criminal justice system should work closely together to ensure that both parties can function optimally.
- The legal department of the SAPS, and the criminal justice system, should investigate the

procedures of section 205, which allows investigators to gain access to the required information, because the process is too slow, and valuable evidence can thus be lost.

- Cyber-crime is not only committed in South Africa. It is committed across the borders of countries, and therefore the SAPS should also consider the procedures that are followed by other countries, to ensure that South Africa is on track with what is going on in the rest of the world. The procedures of the FBI with regard to the quick obtaining of information were mentioned in the research.
- The SAPS should only allow properly trained and skilled cyber-crime investigators to deal with computer evidence, to ensure that the evidence is accepted at the court.

4.4 SUGGESTIONS FOR FURTHER RESEARCH

The researcher is of the opinion that further research is needed in the following aspects:

- Revision of the procedures that are currently followed by investigators to obtain information through Section 205 of the Criminal Procedure Act 51 of 1977.
- Research that will reveal the problems and successes with regard to search and seizure of computer evidence in other countries.
- Research on the modus operandi of cyber-crime offenders in different types of crimes.

4.5 CONCLUSION

Computer seizure as a technique in forensic investigation is the most fundamental stage of computer investigation. Many challenges were established by the research study. It is imperative that the SAPS provide SAPS cyber-crime technicians with adequate training. Various problems, as indicated in the research study, impede progress in the operations of SAPS cyber-crime technicians. The momentum to put into practice the recommendations of this research study, will not only improve the operations of the SAPS cyber-crime technicians, but will uplift the entire criminal justice system.

LIST OF REFERENCES

ACDL Digital Library.2010. *Digital evidence and computer crime*. From: http://prtal.acm.org/citation.cfm? Id=555668 (accessed 27 December 2010).

Afrika, S. 2009.SAPS, *Scorpions in cyber-crimes limbo*. From: http://www.itweb.co.za/sections/internet/2009/09/04281036.asp?=legal%20 (accessed 9 October 2009).

Anson, S. & Bunting, S. 2007. *Mastering windows network forensics and investigation*. Indianapolis, IN: Wiley.

Answerbag. 2010. *Computer Crime Evidence. From*: http://www.answerbag.com/q_view/2012404 (accessed 13 October 2010).

Articlesbase. 2009. *How the computer criminals control information*. From: http://www.articlebase.com/security-articles/computer-criminals-control-inform. (accessed 13 November 2010).

Attack Codes. From: http://en.wikipedia.org/wiki/attack_(computing). (accessed 13 November 2010).

Axelrod, A. & Antinozzi, G. 2003. *Complete guide to criminal investigation*. Indianapolis, IN: Alpha Publishers.

Babbie, E. & Mouton, J. 2002. *The practice of social research*. Cape Town: Oxford University Press.

Bauer, W. & Gaskell, G. 2000. *Qualitative researching with text, image and sound*: practical handbook. London: Sage.

Beginner. From: http://www.ipcbeginner.com/incinfo/trojan-virus.html (accessed 2 October 2010).

Blaikie, N. 2003. *Analyzing qualitative data*. London: Sage.

Bologna, J. 1989. *Forensic accounting handbook*. New York: Wiley.

Bouma, C. D. & Atkinson, G.B.J. 1995. *A handbook of social science research*. Washington: Oxford University Press.

Brenner, S. W. 2009. *Cybercrime*: *criminal threats from cyberspace*. From: http://books.google.co.za/books=drenner+2009+computercrimesource. (accessed 20 September 2010).

Burd, D.S. 1996. *Systems architecture, hardware and software in business information systems*. Cambridge: International Thomson Publishing.

Burrows, T. 2009. *Cyber mafia*. From: http://www.iweek.co.za/viewstory.asp?storyId=197900 (accessed 1 November 2009).

Carter, D. L. 2010. *Computer crime categories*:*how criminals operate*. From: http://www.uplink.com.au/lawlibrary/documents/docs/doc124.html (accessed 11 September 2010).

Casey, E. 2000. *Digital evidence and computer crime*: *forensic science, computers and internet with Cdrom*. Orlando, FL: Academic Press.

Casey, E. 2002. *Handbook of computer crime investigation*. London: Academic Press.

Casey, E. 2003. *Handbook of computer crime investigation*: *forensic tools and technology*. San Diego: Academic Press.

Casey, E. 2004. *Digital evidence and computer crime*. 2nd edition. London: Academic Press.

Casey, E. 2004. *Handbook of computer crime investigation*. New York: Elsevier Academic Press.

Casey, E. & Ferraro, M. M. 2005. *Investigating child exploitation and pornography*. New York: Elsevier Academic Press.

Chunovic, J. 2008. *GSN, Security News*. From: http://www.gsnmagazine.com/category/article-futeres?page 11 (accessed 20 November 2010).

Cisco. 2010. *Support Forums on Computer Crimes*. From: http://supportforums.cisco/thread/17480?+star=O&viewcondensed (accessed 25 September 2010).

Computer Crime. 2010. *Computer Crimes* .From: http://www.holysmoke.org/c00/025.htm (accessed 11 September 2010).

Computer Crime. 2010. *Data alteration*. From: http://www.legacybertips.com/criminallaw-law/computer-crime/computer data alteration (accessed 13 November 2010).

Computer Crime Research Centre. 2005. *Types of computer crime*. From: http://www.crime-research.org/aricles/types-of-computer-crime (accessed 11 September 2010).

Computer Dictionary. 2010. *What is a Computer?* From: http://computer.yourdictinary.com/vandal (accessed 11 October 2010).

Computer Exploits. 2010. *Computer Security Exploits.* From: http//en.wikipedia.org/wiki/*exploit* (computer- security) (accessed 18 October 2010).

Computer Forensics. 2010. *Characteristics and preservation of digital evidence*. From: http://findarticles.comp/articles/mi_192194/25_3_73/ai_n600624 (accessed 27 December 2010).

Computer Forensics. 2010. *Electronic evidence recovery and analysis*. From: http://www.computerforensics.com/faq.html (accessed 27 December 2010).

Computer Forensics. 2010. *Seizing a computer* . From: http://www.priscilla.com/forensics/computerseizure.html (accessed 12 December 2010).

Computer Forensics. 2011. *Computer crime scene investigation*. From: http:11flylib.com/books/en/3.394.1.61/1/ (accessed 1 January 2011).

Computer Forensics World. 2010. *A community of computer forensics professionals*. From: http://www.computerforensicsworld.com (accessed 27 October 2010).

Constitution of the Republic of South Africa Act 108of 1996 (South Africa, 1996). See P96.

Cracker. 2010. *Wireless Cracking*. From: http//en.wikipedia.org/wiki/cracking_of_wireless_networks (accessed 13 November 2010).

Crime Investigation Network. 2010. *Duty description for the crime scene investigator*. From: crime-scene-investigator.netk/dutydescri… (accessed 1 September 2011).

Crime Scene Investigation. 2011. *Presentation transcript*. From: http://www.slideshape.net/crimescenei-investigation (accessed 1 September 2011).

Criminal Procedure Act 51of 1997 of (South Africa, 1977). See P96.

Cross, M. 2008. *Scene of the cybercrime*. 2nd edition. Burlington: Syngress.

Cyber-crime Investigation Cell. 2010. *Forensic computer and cybercrime*. From: http://www.cybercellnumba.com/write-ups/forensics-computer-and-cybercrime. (accessed 13 November 2010).

Davis, C., Philipp, A. & Cowen, D. 2005. *Hacking exposed computer forensics*. New York: McGraw-Hill.

Denial of Service attack. From: http: //en.wikipedia.org/wiki/denial-of-service (accessed 14 November 2010).

Denscombe, M. 1998. *The good research guide for small scale social projects*.

Philadelphia: Open University Press.

Denscombe, M. 2002. *Ground rules for good research*: *a 10-point guide for social researchers*. Philadelphia: Open University Press.

De Vos, A. S. 2002. *Research at grass roots*. 2nd edition. Pretoria: Van Schaik.

eHow. 2011. *How to process a computer crime scene*. From: ehow.com_5832759_process.com (accessed 1 September 2011).

Etter, B. C. 2001. *The challenge of the forensic investigation of computer crime*. From: http://www.afp.gov.au/media/pdf/c/comp-crim (accessed 11 December 2010).

Expert Law. 2004. *Computer forensics*: *data*: *The basics of computer forensics*. From: http://www.expertlaw.com/library/forensics_evidence/basics_forensics.html (accessed 27 October 2010).

Expert Law. 2010. *Computer forensics*. From: http://www.expertlaw.com/library/forensic_evidence/computer_forensics_101leml (accessed 27 October 2010).

Ezine@rticles. 2010. *Types of computer crimes*. From: http://eziearticles.com/?types-of-computer-crimes&id=1017158 (accessed 11 September 2010).

FBI Law Enforcement Bulletin. 2004. *Computer crime*. From: http://www.holysmore.org/c000/025.htm (accessed 11 September 2010).

Field Guide, Part Two.2011. *Investigation of computer crime*. From: http://www.symantec.com/connect/articles/field-guide/part-two (accessed 14 January 2010).

Field Guide ,Part Five.2011.*Search and seizure planning*. From: http://www.symantec.com/connect/articles/field-guide-part-five (accessed 30 January 2011).

Field Guide, Part Six. 2011. *Search and seizure approach, documentation and location*. From: http://www.symantec.com/connect/articles/field-guide-part-six (accessed 24 February 2011).

Fisher, A. J. B. 2004. *Techniques of crime scene investigation*. 7thedition. Boca Raton, FL: CRS Press.

Freedom From Fear Magazine. 2010.*Cyber-crime and organized crime*. From: http://www.freedomfromfearmagazine.org/index.php?optioin=com_content&view=article (accessed 14 November 2010).

Gilbert, J.N. 2004. *Criminal investigation*. 6thedition. Upper Saddle River, NJ: Pearson Prentice

Hall.

Gratton, C. & Jones, I. 2004. *Research methods for sport and studies*. London: Routledge.

Groth, D. & Skandier, T. 2005. *Network + Study guide*.4th edition. Alemeda: Neil Edde Sybex.

Hacker (Computer Security). 2010. *Hacker Computer Security*. From: //en.wikipedia.org/wiki/hacker computer security (accessed 11 September 2010).

Hershensohn, J. 2005. IT forensics: the collection and presentation of digital evidence. From: http://www.e-evidence.infor/h.html (accessed 15 October 2009).

Hofstee, E. 2006. *Constructing a good dissertation*. Sandton: EPE.

Hoyle, R.H., Harris, J.J. & Judd, C.M. 2002. *Research methods in social relations*.7th edition. Pacific Grove: Wadsworth.

Intratec Data Recovery. 2010. *The computer forensic process*. From: http://www.intratec.co.za/computer-forensic.Html?gclid=CNWGs8vR8qCFZRe7A (accessed 27 October 2010).

Johnson, T.A. 2006. *Forensic computer crime investigation*. Chicago: CRC Press.

Journal of American Science. 2010. *Cyber Crime*. From: http://www.americanscience.org (accessed 18 May 2010).

Kabay, M.E. 2008. *Glossary of computer crime terms*. Northfield: Norwich University.

Kenneally. E. 2009. *Confluence of digital and the law*: on the forensic soundness of live-remote digital evidence collections. From: http://www.lawtechjournal.com/articles. (accessed 24 September 2009).

Kipper, G. 2007. *Wireless crime and forensic investigations*. New York: Taylor & Francis.

Kvale, S. 1996. *An introduction in qualitative research intervening*. San Diego, CA: Sage.

Lee, H.C. 2001. *Henry Lee's crime science handbook*. London: Academic Press.

Leedy, P.D. & Ormrod, J.E. 2001. *Practical research*: *planning and design*. Upper Saddle River, NJ: Merrill Prentice Hall.

Leedy, P. D. & Ormrod, J. E. 2005. *Practical research*: *planning and design*. 8th edition. Toronto: Pearson Education.

Logic bomb. 2010. From: *http//en.wikipedia.org/wiki/logic_bomb* (accessed 14 November 2010)

Longman's South African School Dictionary. 2009. s.v." investigation". Cape Town: Longman.

Maat, S.M. 2004. *Cyber-crime*: *comparative law analysis*. From: http://etd.UNISA.oc.za/etd-db/Etd-desk/describe (accessed 12 September 2009).

Mandia, K. & Prosise, C. 2003. *Incident response* &*computer forensics*. 2nd edition. Emeryville, CA: McGraw-Hill.

Marais, C.W. & Van Rooyen, H.J.N. 1992. *Murder investigation*. Silverton: Promedia.

Marcella, A. & Menendez, D. 2008. *Cyber forensics*: *a field manual for collecting, examining and preserving evidence of computer* crimes. 2nd edition. London: Willan.

Mason, J. 1998. Qualitative researching. London: Sage.

Maxfield, M.G. & Babbie, E. 1995. Research methods for criminal justice and criminology. Boston: Wadsworth.

Maxfield, M.G. & Babbie, E. 2001. *Basics of research for criminal and criminology*. 3rd edition. Belmont, CA: Wadsworth.

McAuley, J. 2004. *Managing search and seizures*: From: LEEP://www.KPMG.ca/en/service/advisor/fo (accessed 16 November 2009).

Mendell, R.L. 2004. *Investigating computer crime in the 21st century*. 2nd edition. Springfield: Charles C. Thomas.

Mouton, J. 1996. *Understanding social research*. Pretoria : Van Schaik.

Mouton, J. 2001. *How to succeed in your master's and doctoral studies*. Pretoria:
Van Schaik.

National Cyber Alert System. 2010. *Cyber Crime*. From: http//www.us-cert.gov/cas/tips/st04-015.html (accessed 20 September 2010).

National Institute of Justice. 2010. *Criminal justice research*. From: http://www.nij.gov/ (accessed 19 November 2010).

National Instruction 1/2006 of the SAPS (South African Police Service, 2006). See P96.

Norton. 2010. *Differences between viruses, worms and Trojans*. From: http://service1.symantec.com/support/nav.nsf/90b56492973adccd8825694599552355 (accessed 16 November 2010).

NTI. 2010. *Computer evidence defined*. From: http://www.forensics-intl.com/art18.html (accessed 11 September 2010).

O'Brien, A. J. & Marakas, G.M. 2009. *Management information systems*. 9th edition. New

York: McGraw-Hill.

Oz, E. 2004. *Management information systems*. 4th edition. Great Valley, PA: Pennsylvania State University.

Port Scanner. 2010. *Port Scanners.* From: http://en.wikipedia.org/wiki/port_scanner (accessed 14 November 2010).

Postnote. 2006. Computer Crime. From: http://www.parliament.uk/documtns. (accessed 13 November 2009).

Prevention of Organised Crime Act 121of 1998(South Africa, 1998) see South Africa P93.

Radmin. 2010. *Advanced lanscanner*.From: http://www.radmin.com/products/utilities/lanscanner.php (accessed 26 September 2010).

Robson, C. 2000. *Small-scale evaluation*: principles and practice. London: Sage.

Rude. T. 2000. *Evidence seizure methodology for computer forensics*. From: http://www.crazytrain.com/seizure.html (accessed 30 January 2011).

Search Security. 2010. *War dialer*. From: http://searchsecurity.techtarget.com/sdefinition (accessed 14 September 2010).

Search Software Quality.2010.*Cyber Forensic Software Quality*. From: http://searchsofwarequality.techtarget.com/sdefinition10 (accessed 14 September 2010).

Sheetz, M. 2007. *Computer forensics*: *an essential guide for accountants, lawyers and managers*. Hoboken, NJ: Wiley.

Silvermand, D. 2000. *Doing qualitative research*: *a practical handbook*. London: Sage.

Singleton, R. & Straits, B.C. 1999. *Social research is fundamental*. 3rd edition. New York: Oxford University Press.

Sniffer. 2010. *Sniffer Packet Analyzer*. From: http://en.wikipedia.org/wiki/packet sniffer (accessed 14 November 2010).

South African Government Information. 2008. *Presentation on cyber security*. From: http://www.info.gov.za/speeches/2008/09020414151003.htm (accessed 14 November 2009).

South Africa. 1996. The Constitution of the Republic of South Africa Act 108 of 1996. Pretoria: Government Printer.

South Africa. 1977. Criminal Procedure Act 51 of 1977. Pretoria: Government Printer.

South Africa. 1983. Computer Evidence Act 57 of 1983. Pretoria: Government Printer.

South Africa. 2002. Electronic communications and Transactions Act 25 of 2002. Pretoria: Government Printer.

South Africa. 1998. Prevention of Organised Crime Act 121 of 1998. Pretoria: Government Printer.

South Africa. 2002. Regulation and Provision of Communication Related Information Act 70 of 2002. Pretoria: Government Printer.

South African Pocket Oxford Dictionary. 2002. 3rd edition. Cape Town: Oxford University Press.

South African Police Service. 2006. National Instruction1/2006. Pretoria: Commissioner of the SAPS.

Steel, C. 2006. Windows forensics. Indianapolis, IN: Wiley.

Swanson, C.R., Chamelin, N.C. & Territo, L. 2003. *Criminal investigation*.8th edition. New York: McGraw Hill.

Technology and Lifes tyles. 2010. *Technology lifestyles*. From: http://www.ehow.com/facts_6023233_technology_lifestyles.html (accessed 14 September 2010).

The Computer Forensic Examination Process. 2011. *Computer Crime Examination Steps*. From: http://www.newyorkcomputerforensics_process.php (accessed 25 August 2011).

Tesch, R. 1990. *Qualitative research*: *analysis types* & *software tools*. London: Falmer Press.

Tshwane University of Technology. 2002. *Study guide for investigation of crime* III. Pretoria: The University of Pretoria.

United States. Department of Homeland Security. 2007. *Best practises for seizing electronic evidence*, vol.3: a pocket guide for first responders. Washington, DC: US Secret Service.

United States Secrete Service.2010. Electronic Crimes Task Forces and Working Groups. From: http://www.secretservice.gov/ectf. shtml.

Vacca, J. R. 2002. *Computer forensics*: *computer crime scene investigation*. Hing Ham: Charles River Media.

Viridis, M. 2000. *Computer manipulation crime*. From: http://www.ehow.com/facts_5904206_computer-manipulation-crime_.html (accessed 13 November 2010).

Webopedia Computer Dictionary. 2010. *Cryptanalysis*. From:

http://www.webopedia.com/term/c/cryptanalysis.html (accessed 14 November 2010).

Welman, J. C. & Kruger, S. J. 2001. *Research methodology*. 2nd edition. Cape Town: Oxford University Press Southern Africa.

Welman, J. C. & Kruger, S. J. 2002. *Research methodology for the business and administrative sciences*. 2nd edition. Cape Town: Oxford University Press Southern Africa.

Welman J. C., Kruger, S. J. & Mitchell, B. 2005. *Research methodology*. 3rdedition. Johannesburg: Thomson Publishers.

Wiles, J., Cardwell, K. & Reyes, A. 2007. *The best damn cybercrime and digital forensics.* Burlington: Syngress Publishing..

wiseGEEK. *Computer evidence*. From: http://www.wisegeek.com/what_is_computer_evidence.htm (accessed 26 December 2010).

Your Dictionary. 2010. *Vandal-computer dictionary definition*. From: http://computer.yourdictionary.com/vandal (accessed 13 November 2010).

ANNEXURE A

INTERVIEW SCHEDULE: CYBER-CRIME TECHNICIANS

COMPUTER SEIZURE AS TECHNIQUE IN FORENSIC INVESTIGATION

Section A: Background Information

1. To what unit are you attached?
2. What is your current position in the unit?
3. How long have you been in this unit?
4. Have you undergone or received formal training with regard to seizure of computers?
5. If the answer to the previous question is 'yes', please explain what type of training you received.
6. To what degree have you formerly dealt with the seizure of computers?

Section B: The role of a computer to facilitate the commissioning of crimes in forensic investigation

7. What is forensic investigation?
8. Is there any difference between forensic investigation and criminal investigation?
9. If the answer to the previous question is 'yes', briefly explain the difference.
10. What is the role of computers in facilitating the commissioning of crimes in forensic investigation?
11. What are the objectives of forensic investigation?
12. What is the role of computer evidence in forensic investigation?
13. What are the types of evidence pertaining to computers?
14. What are the types of crimes associated with computers?
15. What are the phases of computer investigation?

Section C: Seizing computers without compromising evidence

16. In a case where it is necessary to seize a computer, explain briefly what type of person you

think should seize a computer.

17. What, in your opinion, would you consider to be a challenge in seizing computer evidence?
18. Do you have any suggestions to solve these problems?
19. What impact would a crime scene with a huge storage capacity have on the ability of the investigator?
20. Are you in possession of a set of rules or guidelines to deal with a computer crime scene?
21. If the answer to the previous question is ‘yes’, what are those guidelines?
22. What are the legal guidelines to keep in mind when seizing computer evidence?
23. Is there a set of tools required to seize or collect computer evidence?
24. If the answer to the previous question is ‘yes’, what are those tools?
25. What should be seized for the retrieval of computer evidence?
26. Why is it important to maintain a chain of custody of computer evidence?
27. How would the removal of power from a running system impact on the stored evidence?
28. Taking storage after seizure into consideration, under what conditions should the computer equipment be stored?
29. Is there a possibility that storage devices may not be located on the premises where the seizure is conducted?
30. If the answer to the previous question is ‘yes’, please explain what the steps will be to take.

ANNEXURE B

INTERVIEW SCHEDULE: PROSECUTORS

COMPUTER SEIZURE AS TECHNIQUE IN FORENSIC INVESTIGATION

Section A: Background Information

1. What is your occupation?
2. For how long have you been a prosecutor?
3. How many years of experience do you have in prosecuting cyber-crimes?
4. How often do you prosecute cyber-crime cases?
5. Did you receive any training in the prosecution of cyber-crime cases?

Section B

6. What, in your opinion, are the legal challenges that investigators have to deal with when seizing computers?
7. Are there any challenges that are facing South African legislation in terms of regulating cyber- crimes?
8. What is your role as prosecutor when dealing with investigators who are responsible for a cyber-crime investigation?
9. Currently, would you consider cyber-crime investigators as successful? Please motivate your answer.
10. In your opinion, what could be done to improve the success rate of cyber-crime prosecutions?
11. Are cyber-crimes different from other types of crimes?
12. If the answer to the previous question is ‘yes’, explain the difference.
13. Is there any important legislation that, in your opinion, cyber-crime investigators should be familiar with?
14. If your answer is ‘yes’, please elaborate.

ANNEXURE C

APPROVAL TO CONDUCT RESEARCH

14-DEC-2010 11:02 FROM DIV COM CI TO 0437434060 P.01/02

South African Police Service **Suid-Afrikaanse Polisiediens**

Private Bag / Privaatsak	X301	Fax no / Faks no	(012) 347 3050
YOUR REFERENCE / U VERWYSING	3/34/2	DIVISIONAL COMMISSIONER CRIME INTELLIGENCE HEAD OFFICE PRETORIA 0001	
MY REFERENCE / MY VERWYSING			
ENQUIRIES / NAVRAE	Lt Gen Mdluli Brigadier (Dr) BM Zulu		
TEL.NO	(012) 360 1398		
		13 December 2010	

The Head
Strategic Management
South African Police Service
HEAD OFFICE

RE: RESEARCH PROPOSAL : COMPUTER CRIMES AS SEIZURE TECHNIQUE IN FORENSIC INVESTIGATION : M-TECH IN FORENSIC INVESTIGATION: UNIVERSITY OF SOUTH AFRICA: RESEARCHER: LT COL VUYANI NDARA

1. Your letter dated 2010-11-11 with reference number 3/34/2 on the above subject has bearing on this matter.

2. The Divisional Commissioner: Crime Intelligence hereby approves the study in principle based on the following conditions:

2.1 The research should be knowledge based which will be based on the responses that will verbally be provided by respondents. Due to adherence to Security Standard principles of Intelligence, no evidence should be collected during interviews. The collection of data through utilisation of Intelligence Systems is not permitted during the research process.

2.2 All the structured questionnaires that have been approved by the supervisor / promoter of the study to be asked during the interviews must be forwarded for to the Divisional Commissioner: Crime Intelligence so that he can check if respondents will not breach any Security Standards in terms of information sharing when responding to the questions.

2.2 The researcher must write the letter in advance to the Divisional Commissioner: Crime Intelligence, notifying him of the dates of interviews as well as the names of your targeted sampled population in order for the Divisional Commissioner to give approval to your target population to respond on your questions.

2.3. Information obtained during the research process should only be utilised for research study purpose only.

3. This office will like to wish Lt Col Ndara a good luck in his studies.

LIEUTENANT GENERAL
DIVISIONAL COMMISSIONER: CRIME INTELLIGENCE
R.N. MDLULI (SOE)

ANNEXURE D

EDITOR'S CERTIFICATE

20 February 2013

I, Marlette van der Merwe, ID 4802060118085, hereby certify that the master's dissertation, "Computer seizure as technique in forensic investigation", by Vuyani Ndara, has been edited by me, according to the referencing method used by Unisa.

Marlette van der Merwe - BA, HDipLib (UCT)

Member: Professional Editors' Group